Groupe de travail Réseau
Request for Comments : 2652
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

J. Allen, WebTV Networks, Inc.
M. Mealling, Network Solutions, Inc.
août 1999

Définitions d'objets MIME pour le protocole d'indexation commune (CIP)

Résumé
Le protocole d'indexation commune (CIP, *Common Indexing Protocol*) est utilisé pour passer les informations d'indexation de serveur à serveur afin de faciliter l'acheminement des interrogations. Le protocole se compose de plusieurs objets MIME qui sont passés de serveur à serveur. Le présent document décrit les définitions de ces objets ainsi que les méthodes et exigences nécessaires pour définir un nouveau type d'indice.

Table des Matières

1. Introduction

Le protocole d'indexation commune (CIP, *Common Indexing Protocol)* est utilisée pour passer des indices entre des serveurs qui combinent plusieurs indices et/ou acheminent les interrogations sur la base de ces indices. Le cadre global de ce protocole est spécifié dans le document cadre de CIP [RFC2651]. Le présent document devrait être lu dans le contexte de ce document car il y a des concepts fondamentaux qui sont contenus dans le cadre et dont l'explication n'est pas reprise ici.

Comme il y a différentes façons d'indexer une certaine base de données, il y aura aussi plusieurs types d'indices à passer. Ces indices peuvent avoir des exigences de transport différentes, différentes façons de spécifier les paramètres, et différentes règles de référents. Ces exigences différentes sont traitées en encapsulant les indices au sein d'enveloppeurs MIME afin d'avoir une façon normalisée de spécifier ces différents paramètres.

L'Appendice A contient les gabarits réels d'enregistrement MIME [RFC2046] envoyés à l'IANA pour l'enregistrement [RFC2048].

Le présent document utilise des mots comme DEVRAIT et DEVRA qui ont une signification particulière spécifiée dans "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence" [RFC2119].

2. Transactions CIP

Les messages passés par les mises en œuvre CIP sur des mécanismes de transport fiable entrent dans trois catégories : les demandes, les réponses et les résultats. Toutes les demandes résultent soit en une réponse, soit en un résultat. Un résultat envoyé en réponse à une demande doit être interprété comme une opération réussie.

Les demandes, les réponses et les résultats sont formatés comme des messages MIME [RFC2046]. Les types MIME spécifiques impliqués sont définis ci-dessous.

Comme avec tous les objets MIME, les messages CIP peuvent être enveloppés dans un paquetage multiparties de sécurité pour assurer l'authentification et la confidentialité. La politique de sécurité à l'égard de tous les messages est définie par la mise en œuvre, lorsque elle n'est pas explicitement discutée ci-dessous. Les mises en œuvre CIP sont fortement invitées à permettre aux administrateurs de serveur une possibilité maximum de configuration pour sécuriser leurs serveurs contre les messages CIP anonymes malveillants. En général, les opérations qui peuvent changer de façon permanente l'état du serveur d'une façon dommageable ne devraient avoir lieu qu'à réception d'un message correctement signé d'un homologue CIP de confiance ou d'un administrateur. Les mises en œuvre devraient fournir des capacités d'analyse appropriées afin que les demandes aussi bien réussies que défaillantes puissent être suivies par l'administrateur du serveur.

Comme ces objets MIME peuvent être et seront envoyés sur plusieurs protocoles différents, les terminaisons de corps sont spécifiées par le protocole de transfert. Les nouveaux protocoles sont invités à utiliser la terminaison de corps de style SMTP [RFC0821].

Finalement, comme les objets MIME peuvent spécifier leur propre codage, les fins de ligne contenus dans chaque corps sont définis par le codage. Donc, au lieu de les spécifier comme retour chariot et/ou saut à la ligne, on utilisera l'identifiant <fin de ligne>. Les fins de ligne dans les en-têtes et la séparation du corps des en-têtes suivent les normes existantes.

2.1 Définitions syntaxiques communes

Certains éléments syntaxiques sont communs à toutes les transactions CIP. Cela inclut le type, le DSI et l'URI de base.

2.1.1 Arborescence de type MIME "application/index"

Du fait des exigences de la RFC2048 concernant les objets qui ont le même type mais des syntaxes différentes, les objets CIP vont utiliser l'arborescence application/indice mais inclure des "facettes" [RFC2048] qui l'étendent comme l'ont fait d'autres types par rapport aux éléments globaux et aux améliorations spécifiques des fabricants. Donc, l'arborescence est divisée selon les branches suivantes :

application/index.cmd._command_
application/index.response
application/index.obj._type_
application/index.vnd._xxx_

command est une commande comme spécifié ici. Il contient les commandes et leurs arguments.

type identifie le type d'objet d'indice CIP contenu dans le corps. Il est unique parmi tous les autres types réservés.
Les types réservés sont ceux qui ont été précédemment documentés par d'autres spécifications d'objet d'indice CIP, selon le processus de normalisation de l'IETF.

xxx est un identifiant spécifié par un fabricant qu'il va utiliser dans des opérations spécifiques des indices.

Tous les identifiants ci-dessus suivent les règles de la [RFC2048] pour les types MIME valides. De plus, les commandes, les réponses et les types sont limités par le présent document à comporter de 1 à 20 caractères de l'ensemble [a-zA-Z0-9-] ; c'est-à-dire, toutes les lettres majuscules et minuscules, tous les chiffres, et le caractère ASCII moins (décimal 45). Bien que les noms de types puissent être spécifiés comme insensibles à la casse, ils doivent être comparés et traités par ailleurs sans considération de la casse.

L'Appendice A contient le gabarit d'enregistrement pour l'arborescence application/indice.

2.1.2 DSI

Un identifiant d'ensemble de données (DSI, *dataset identifier*) est un identifiant choisi dans toute partie de l'espace d'OID ISO/CCITT. Le DSI identifie de façon univoque un certain ensemble de données parmi tous les ensembles de données indexés par CIP.

Comme ils sont actuellement définis, les OID sont une séquence non bornée d'entiers non bornés. Bien que cela crée un espace de numérotation infini, cela pose des problèmes aux mises en œuvre qui ont affaire à des machines qui ont des ressources finies. Pour faciliter la mise en œuvre, le présent document spécifie un codage ASCII de l'OID, et spécifie des limites qui rendent plus facile la mise en œuvre.

Pour les besoins des échanges de messages CIP, un OID doit se conformer aux règles suivantes :

```
dsi             = entier *( "." entier)
entier          = tous-chiffres / (un-à-neuf *tous-chiffres)
un-à-neuf       = "1" / "2" / "3" / "4" / "5" / "6" / "7" / "8" / "9"
tous-chiffres   = "0" / un-à-neuf
```

En aucune circonstance la longueur totale de la chaîne résultante ne doit excéder 255 caractères. Les OID qui ne peuvent pas, à cause de leur longueur, se conformer à ces règles ne doivent pas être utilisés comme identifiants d'ensemble de données CIP.

Une mise en œuvre ne doit pas tenter d'analyser les entiers individuels sauf si elle est prête à traiter des entiers de longueur arbitraire. Traiter le DSI comme autre chose qu'une chaîne opaque de caractères US-ASCII n'est pas recommandé.

Deux DSI CIP sont considérés comme correspondants si tous deux se conforment aux règles ci-dessus et si chaque nombre correspond.

2.1.3 Base-URI

Les objets d'indice CIP portent des URI de base pour faciliter la génération de référents sur la base de l'objet d'indice. Le paramètre base-URI porte une liste d'URL délimités par des espaces. Les URL sont définis dans la [RFC1738]. Les règles exactes sont les suivantes :

```
base-uri      = genericurl *( 1*whitespace genericurl )
whitespace    = "<space>" (decimal 32) / "<tab>"   (decimal 9)  / "<cr>"    (decimal 13) / "<lf>"    (decimal 10)
genericurl    = { comme spécifié dans la [RFC1738], section 5 }
```

2.2 Format de réponse

Toutes les demandes doivent être suivies d'un code de réponse, sauf dans les cas où un chemin de retour n'est pas disponible.

La définition de ce type MIME est :

```
Nom du type MIME :          application
Nom du sous-type MIME :     index.response
Paramètres exigés :         code
Paramètres facultatifs :    jeu de caractères
Considérations de sécurité : (Voir la Section 4)
```

Le paramètre code contient un code de retour de trois chiffres qui note l'état de la dernière commande.

Le format du corps est tel que la première ligne est interprétée comme le commentaire correspondant au code. Comme avec la plupart des codes de réponse, ce commentaire est destiné au lecteur humain et peut ne pas exister et ne doit pas dépendre du protocole. Les lignes suivantes dans le corps sont réservées pour que chaque réponse les définisse. Dans le cas où le

commentaire n'est pas donné, la première ligne doit être vide.

body = comment linebreak payload
comment = { tout texte }
linebreak = (decimal 13) (decimal 10)
payload = { tout texte }

Le paramètre charset a la signification MIME normale. Voici plusieurs exemples :

[begin MIME]
Content-type: application/index.response; code=220

CIP Server v1.0 ready!<fin de ligne>
[end MIME]

[begin MIME]
Content-type: application/index.response; code=500

MIME formatting problem<fin de ligne>
[end MIME]

[begin MIME]
Content-type: application/index.response; code=520

<fin de ligne>
[end MIME]

Bien que les réponses décrites dans ce document n'utilisent pas le reste des lignes dans le corps d'une réponse, les mises en œuvre devraient veiller à ne pas l'interdire à l'avenir. Un bon exemple serait un message spécifiant qu'une demande d'interrogation ne contenait pas les attributs exigés. Ce message ressemblerait à ceci :

[begin MIME]
Content-type: application/index.response; code=502

Il manque à la demande les attributs CIP requis
Missing-Attribute: attribute1Missing-Attribute: attribute2
Missing-Attribute: attribute3
[end MIME]

La signification des divers chiffres dans les codes de réponse est exposée à l'Appendice E de la [RFC0821].

Voir à l'Appendice B la liste des codes de réponse valides.

2.3 Format de commande

Une commande CIP initie soit un transfert d'indice, soit interroge l'état du receveur CIP (ou la participation du serveur dans le maillage) soit change l'état du serveur (ou la place du serveur dans le maillage).

Les commandes CIP sont envoyées comme un message MIME du type "application/index.cmd._command_". La définition de cette arborescence de type est la suivante :
Nom de type MIME : application
Nom de sous-type MIME : index.cmd._command_
Paramètres facultatif : type, dsi
Considérations de sécurité : (Voir la Section 4)

Le format du corps est défini par chaque commande. Une orientation générale de paire attribut/valeur est conservée tout au long des commandes spécifiées suivantes. Ceux qui développent de futures commandes devraient tenter de conserver cette orientation mais ils ne sont pas obligés de le faire.

Dans les paragraphes qui suivent, la réponse du serveur pour chaque valeur possible pour "command" est définie. Noter que les paramètres désignés ci-dessus comme facultatifs ne le sont que par rapport à la forme MIME générique. Les paramètres facultatifs ne le sont que par rapport à l'analyse MIME. Si un ou plusieurs des paramètres nécessaires pour satisfaire une

commande manquent, un code de réponse de 502 est retourné.

Les paramètres facultatifs supplémentaires qui ne sont pas reconnus doivent être ignorés en silence.

2.3.1 No-operation

Nom de commande : application/index.cmd.noop
Paramètres exigés : (aucun)

Une commande CIP avec le paramètre "command" réglé à "noop" doit être acquittée avec le code de type de réponse de 200 (commande OK, pas de réponse à venir).

Cette commande ne doit pas exiger un objet MIME signé. Les mises en œuvre devraient accepter les commandes qui ont été valablement signées.

Exemple :

[begin MIME]
Content-type: application/index.cmd.noop

[end MIME]

Noter l'absence de corps mais que la paire <fin de ligne> est toujours préservée après l'en-tête Content-type.

2.3.2 Poll

Nom de demande : application/index.cmd.poll
Paramètres exigés : type, dsi

La commande "poll" est utilisée par un interrogateur pour demander le transfert d'un objet d'indice. Elle exige les paramètres suivants :

type : Type d'objet d'indice demandé
dsi : Ensemble de données que l'indice devrait couvrir

Si il n'y a pas d'objet d'indice disponible pour un certain DSI, ou si le receveur CIP ne prend pas en charge un certain type d'objet d'indice, le receveur CIP doit répondre par le code de réponse 200, (réussite, pas de réponse à venir). Autrement, le code de réponse doit être 201 (réussite, une réponse arrive).

La politique de sécurité pour les commandes poll est entièrement définie par la mise en œuvre. Les mises en œuvre peuvent être configurées à accepter ou rejeter les commandes poll anonymes.

Exemple :

[begin MIME]
Content-type: application/index.cmd.poll; type="simple"; dsi= "1.3.5.7.9"

Template: nom adresse téléphone du contact<fin de ligne>
Start-time: Fri May 30 14:25:30 EDT 1997<fin de ligne>
End-time: Sat May 31 14:25:30 EDT 1997<fin de ligne>
[end MIME]

2.3.3 DataChanged

Nom de demande : application/index.cmd.datachanged
Paramètres exigés : type, dsi

La commande "datachanged" est utilisée par un interrogé pour notifier à un interrogateur que les données au sein d'un indice ont changé. Elle exige les paramètres suivants :

type : Type d'objet d'indice demandé
dsi : Ensemble de données que l'indice devrait couvrir

Si il n'y a pas d'objet d'indice disponible pour un certain DSI, ou si le receveur CIP ne prend pas en charge un certain type d'objet d'indice, le receveur CIP doit répondre avec le code de réponse 200, (réussite, pas de réponse à venir). Autrement, le code de réponse doit être 201 (réussite, la réponse arrive).

Le corps d'une commande DataChanged est formaté comme un simple ensemble de paires de valeurs d'attribut suivant les règles de la [RFC0822]. Les attributs et valeurs réels admis sont définis par spécification du type d'indice.

La politique de sécurité pour les commandes DataChanged est entièrement définie par la mise en œuvre. Les mises en œuvre peuvent être configurées à accepter ou rejeter les commandes DataChanged anonymes.

Exemple :

[begin MIME]
Content-type: application/index.cmd.datachanged; type="simple"; dsi= "1.3.5.7.9"<linebreak>

Time-of-latest-change: Fri May 30 14:25:30 EDT 1997<fin de ligne>
Time-of-message-generation: Fri May 30 14:25:30 EDT 1997<fin de ligne>
Host-Name: cip.rwhois.net<fin de ligne>
Host-Port: 4322<fin de ligne>
Protocol: RWhois2.0<fin de ligne>
[end MIME]

2.3.4 Demandes supplémentaires

Les demandes spécifiées ci-dessus sont celles qui sont exigées pour mettre en œuvre un maillage simple. On s'attend à ce que d'autres demandes soient développées pour traiter les problèmes de gestion de maillage et les demandes de collecte de statistiques. C'est un point qui devra faire l'objet de travaux complémentaires. Précisément, d'autres travaux sont nécessaires dans le domaine de la gestion des maillages car ceux-ci vont tendre à être organisés autour des caractéristiques de leur type d'indice.

2.4 Format d'objet d'indice

En réponse à la commande "poll", un serveur peut choisir d'envoyer un ou plusieurs objets d'indice. Sans considération du nombre d'objets d'indice retournés, la réponse doit prendre la forme d'un message MIME multipartie/mixte. Chaque partie doit elle-même être un objet MIME du type "application/index.obj._type_". Voici la définition pour ce type :

Nom de type MIME :	application
Nom de sous-type MIME :	index.obj._type_
Paramètres exigés :	dsi, base-uri
Paramètres facultatifs :	aucun
Considérations de sécurité :	(Voir la Section 4)

Comme on l'a décrit précédemment, chaque objet d'indice est d'un type particulier. Ce type est spécifié dans le nom de sous-type MIME car certains types peuvent avoir une syntaxe différente.

Les paramètres exigés sont à utiliser comme suit :

DSI : Le DSI est une chaîne qui identifie mondialement de façon univoque l'ensemble de données à partir duquel l'indice a été créé.

base-URI : Un ou plusieurs URI vont former la base de tout référent créé sur la base de cet objet d'indice.

3. Exigences pour la définition d'un type d'indice

À cause du besoin d'indices spécifiques du domaine d'application, les objets d'indice CIP sont abstraits ; ils doivent être définis par une spécification distincte. Les protocoles de base pour déplacer les objets d'indice sont largement applicables, mais le concept spécifique de l'indice, et la structure du maillage de serveurs qui passent un type particulier d'indices dépend du domaine d'application. Bien que des documents d'accompagnement doivent décrire les objets d'indice, il y a un ensemble d'exigences et de questions de base que ces documents doivent traiter. Cela est destiné à assurer que les hypothèses de base du protocole CIP sur les indices peuvent réellement être exprimées au sein de l'indice.

Comme chaque type est un type MIME par lui-même, l'enregistrement de nouveaux types suit les politiques d'enregistrement standard spécifiées dans la [RFC2048].

3.1 Demandes spécifiques d'un type

Toute définition de type d'indice doit traiter des corps spécifiques du type des demandes Poll et DataChanged. Tous les paramètres inclus dans le corps doivent être spécifiés.

3.2 Paramètres index.obj

3.2.1 Type

Voir les définitions ci-dessus pour les valeurs admises pour le type.

Un nouveau nom doit être alloué lorsque des changements au document qui décrit le type de l'objet d'indice ne sont pas complètement rétrocompatibles.

3.2.2 DSI

Un autre attribut est le "DSI", ou Identifiant d'ensemble de données, qui identifie de façon univoque l'ensemble de données à partir duquel l'indice a été créé. La spécification de l'indice devrait définir les politiques sur la façon dont le DSI est généré. Cela inclut le concept de ce que signifie un ensemble de données pour l'indice concerné.

3.2.3 Base-URI

Un attribut de l'objet d'indice qui est crucial pour générer les référents est le "Base-URI". Le ou les URI contenus dans cet attribut forment la base de tout référent généré sur la base de ce bloc d'indice. L'URI est aussi utilisé comme entrée durant le processus d'agrégation d'indices pour restreindre les types possibles d'agrégation. Cet usage du Base-URI est en rapport avec les maillages qui acceptent plusieurs protocoles.

Donc, une spécification d'indice devrait définir comment le Base-URI s'applique à l'indice sous-jacent et comment il est changé durant le processus d'agrégation.

3.3 Agrégation

Toutes les spécifications d'objet d'indice doivent traiter la question de l'agrégation. C'est la méthode par laquelle un serveur d'indices prend deux indices ou plus et les combine en un indice à passer. Il n'est pas exigé qu'un certain type d'indice s'agrège. Si il ne le fait pas, elle doit explicitement en mentionner les raisons et les effets que cela a sur l'adaptabilité.

Si un certain indice s'agrège, l'algorithme pour cette agrégation doit être donné. Elle doit aussi régler comment cet algorithme affecte l'organisation et l'adaptabilité du maillage.

Les auteurs de document d'objet d'indice devraient se rappeler que tous les types d'agrégation devraient être effectués sans compromettre la capacité à acheminer correctement les interrogations tout en évitant de manquer un nombre excessif de résultats. La probabilité acceptable de faux négatifs doit être établie sur la base du domaine d'application, et est contrôlée par la granularité de l'indice et les règles d'agrégation définies pour lui par la spécification particulière.

Rien dans le présent document n'interdit spécifiquement les règles d'agrégation qui traitent de différents types d'objet d'indice. Ce type de maillage hétérogène est difficile à formuler au mieux et n'est donc pas couvert par ces documents. Si les auteurs de documents souhaitent tenter un tel maillage, ils devraient être conscients que ceci est considéré comme un concept mal compris qui contient de nombreux pièges pour le constructeur de maillage.

3.4 Sémantique de la génération de référent

Comme la méthode par laquelle un client navigue sur le maillage est par référents, le document doit traiter comment un certain protocole d'accès génère un référent à partie de l'indice. Les auteurs devraient prêter une attention particulière au cas où un indice est accédé par différents protocoles et aux interactions entre eux. Par exemple, un indice qui prend en charge des référents qui sont générés à la fois par RWhois et LDAP doit comprendre que l'un utilise un nom distinctif et pas l'autre. L'impact de ces différences sur le référent devrait être clair.

3.5 Sémantique de la confrontation

La décision de générer ou non un référent doit être traitée par le protocole d'accès. La sémantique qui entoure cette décision a un grand impact sur l'efficacité des recherches ainsi que sur les exigences d'agrégation. Donc, les auteurs de spécification d'indice doivent être très clairs sur la façon dont une correspondance est déterminée.

3.6 Considérations pour la sécurité

Comme il est de coutume avec la documentation de protocole Internet, une brève revue des implications pour la sécurité de l'objet proposé doit être incluse. Cette section peut devoir faire un peu plus que de faire écho aux considérations exprimées dans la section des considérations de sécurité du présent document.

3.7 Couverture facultative

Parce que les algorithmes d'indexation, les technologies de listes d'arrêt et de réduction des données, sont considérées par certains concepteurs d'objet d'indice comme étant leur propriété, il n'est pas nécessaire de discuter des processus utilisés pour déduire les informations d'indexation d'un corps de matériaux de source. Lorsque des technologies d'indexation brevetées sont utilisées dans un maillage public, tous les serveurs CIP dans le maillage devraient être capables d'analyser l'objet d'indice (et d'effectuer les opérations d'agrégation si nécessaire) bien qu'il ne soit pas nécessaire que tous soient capables de créer ces indices brevetés à partir des données de source.

Donc, les concepteurs d'objet d'indice peuvent choisir de rester silencieux sur les algorithmes utilisés pour générer les indices, pour autant qu'ils documentent de façon adéquate comment participer à un maillage de serveurs qui passent ces indices brevetés.

Les concepteurs devraient aussi envisager d'inclure des exemples utiles de données de source, de l'indice généré, et les résultats attendus des exemples de confrontations. Lorsque l'algorithme d'agrégation est complexe, il est recommandé que soit inclus un tableau montrant deux indices et l'indice agrégé résultant.

4. Considérations pour la sécurité

Les considérations de sécurité entrent en jeu dans au moins les deux scénarios qui suivent. Les informations d'indexation peuvent laisser échapper des quantités indésirables d'informations protégées par un brevet, si elles ne sont pas contrôlées avec soin. À un niveau plus fondamental, le protocole CIP lui-même exige des services de sécurité externes pour fonctionner de manière sûre. Ces deux sujets sont traités ci-dessous.

4.1 Indexation sûre

CIP est conçu pour indexer toutes les sortes de données. Certaines de ces données peuvent être considérées comme précieuses, protégées par un brevet, ou même très sensibles, par le détenteur des données. Prenons, par exemple, une base de données de ressources humaines. Il peut par contre être très utile pour une société de rendre publics certains éléments de données. Cependant, la base de données dans sa totalité est un actif très précieux, que la société doit protéger. On a gagné au fil des ans beaucoup d'expérience dans la communauté des services d'annuaire sur la meilleure façon de tenir le cap entre la révélation complète de la base de données et la publication des parties utiles.

Un autre exemple où la sécurité devient un problème pour un éditeur de données qui aimerait participer à un maillage CIP. Les données que crée et gère l'éditeur son le principal capital de l'entreprise. Il y a une incitation financière à participer à un maillage CIP, car exporter les indices des données va rendre plus probable que des gens fassent des recherches dans votre base de données. (Tirer un profit de l'activité de recherche est un des objectifs de l'entrepreneur.) Là encore, l'indice doit être conçu avec soin pour protéger la base de données tout en fournissant un synopsis utile des données.

Une des bases de CIP est que les fournisseurs des données vont vouloir fournir des indices de leurs données aux serveurs d'indexation homologues. Sauf si ils sont construits avec soin, ces indices pourraient constituer une menace pour la sécurité de la base de données. Donc, la sécurité des données doit être une considération première lors du développement d'un nouveau type d'objet d'indice. Le risque d'un détricotage d'une base de données sur la seule base des indices exportés à partir d'elle doit être gardé à un niveau cohérent avec la valeur des données et du besoin d'une granularité fine de l'indexation.

Comme CIP est codé comme les objets MIME, les solutions de sécurité de MIME devaient être utilisées chaque fois que possible. Précisément, lorsque il s'agit de la sécurité entre les serveurs d'indices.

4.2 Sécurité du protocole

Les échanges du protocole CIP, qui prennent la forme de messages MIME, peuvent être sécurisés en utilisant toute technologie disponible pour sécuriser les objets MIME. En particulier, l'utilisation des multiparties de sécurité de la [RFC1847] est recommandée. Une application solide de la [RFC1847] utilisant un logiciel de chiffrement largement disponible est PGP/MIME, de la [RFC2015]. Les mises en œuvre sont invitées à prendre en charge PGP/MIME, car c'est la première application viable de l'architecture de multiparties de sécurité de MIME. Lorsque d'autres technologies seront disponibles, elles pourront être incorporées dans le maillage CIP.

Si une demande entrante n'a pas une signature valide, elle doit être considérée comme anonyme pour les besoins du contrôle d'accès. Le serveurs peuvent choisir de permettre certaines demandes provenant d'homologues anonymes, en particulier lorsque la demande ne peut pas causer de dommages permanents au serveur local. En particulier, répondre à des demandes d'interrogation anonymes encourage les constructeurs d'indices à interroger un serveur, faisant mieux connaître les ressources du serveur.

La politique de sécurité explicite par rapport aux demandes entrantes sort du domaine d'application de la présente spécification. Les mises en œuvre ont toute liberté pour accepter ou rejeter toute demande sur le fondement des attributs de sécurité du message entrant. Lorsque une demande est rejetée pour des raisons d'authentification, un code de réponse de la série 530 doit être produit.

Remerciements

Merci aux nombreux membres du groupe de travail FIND qui nous ont aidé par les discussions qui ont conduit à la présente spécification.

Des remerciements particuliers sont adressés à Jeff Allen, anciennement de Bunyip Information Systems. La version d'origine de ces documents a énormément aidé à cristalliser le débat et le consensus. La plus grande partie du texte du présent document a été rédigée à l'origine par Jeff.

Adresse des auteurs

Jeff R. Allen
246 Hawthorne St.
Palo Alto, CA 94301
USA
mél : jeff.allen@acm.org

Michael Mealling
Network Solutions, Inc.
505 Huntmar Park Drive
Herndon, VA 22070
téléphone : 703-742-0400
mél : michael.mealling@RWhois.net

Références

[RFC0821] J. Postel, "Protocole simple de transfert de messagerie", STD 10, août 1982.

[RFC1847] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Sécurité multiparties pour MIME : multipartie/signée et multipartie/chiffrée", octobre 1995. *(P.S.)*

[RFC2015] M. Elkins, "Sécurité de MIME avec Pretty Good Privacy (PGP)", octobre 1996. (*MàJ par* RFC3156) *(P.S.)*

[RFC2046] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 2 : Types de support", novembre 1996. *(D. S., MàJ par 2646, 3798, 5147, 6657.)*

[RFC2048] N. Freed, J. Klensin et J. Postel, "Extensions multi-objets de la messagerie Internet (MIME) Partie 4 : Procédures d'enregistrement", BCP 13, novembre 1996. *(Rendue obsolète par les RFC 4288-4289)*

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

[RFC2651] J. Allen, M. Mealling, "Architecture du protocole d'indexation commune (CIP)", août 1999. *(P.S.)*

Appendice A Gabarits d'enregistrement de type de support

Les gabarits suivants ont été enregistrés auprès de l'IANA :

Arborescence d'indice

To: ietf-types@iana.org
Subject: Enregistrement d'une arborescence de type de support MIME d'application/indice

Nom de type de support MIME : application
Nom de sous-type MIME : indice
Paramètres exigés : aucun
Paramètres facultatif : aucun
Considérations de codage : aucune
Considérations de sécurité : Les considérations de sécurité entrent en jeu au moins dans les deux scénarios suivants. Il peut y avoir des fuites sur des quantités d'informations d'indexation non désirées sur des éléments confidentiels si elles ne sont pas contrôlées avec soin. À un niveau plus fondamental, le protocole CIP lui-même exige des services externes de sécurité pour fonctionner de manière sûre. Les deux sujets sont traités ci-dessous.
Considérations d'interopérabilité :
Spécification publiée : RFC 2652
Applications qui utilisent ce type de support : Ce type de support est utilisé pour contenir des informations sur des indices et la façon dont ils interopèrent pour former des maillages de serveurs d'indices.
Informations supplémentaires : Ce type de support n'est pas un type autonome. C'est le niveau supérieur d'une arborescence similaire aux arborescences vnd ou prs spécifiées au paragraphe 2.1 de la [RFC2048]. Il y a quatre branches spécifiées dans cette arborescence :

application/index.cmd
application/index.response
application/index.obj
application/index.vnd

Chacune de ces branches est une arborescence de plein droit avec des types enregistrés en dessous d'elles. Voir les enregistrements pour plus d'informations sur les types permis en dessous de ces embranchements.

Adresse personnelle et de messagerie à contacter pour des informations complémentaires :
Utilisation prévue : UTILISATION LIMITÉE
Auteur/contrôleur des modifications :

Arborescence des commandes

To: ietf-types@iana.org
Subject: Enregistrement d'une arborescence de type de support MIME application/index.cmd

Nom de type de support MIME : application
Nom de sous-type MIME : index.cmd
Paramètres exigés : aucun
Paramètres facultatif : aucun
Considérations de codage : aucune
Considérations de sécurité : Les considérations de sécurité entrent en jeu au moins dans les deux scénarios suivants. Il peut y avoir des fuites sur des quantités d'informations d'indexation non désirées sur des éléments confidentiels si elles ne sont pas contrôlées avec soin. À un niveau plus fondamental, le protocole CIP lui-même exige des services externes de sécurité pour fonctionner de manière sûre. Les deux sujets sont traités ci-dessous.
Considérations d'interopérabilité : Les mises en œuvre devraient traiter les commandes inconnues avec douceur.
Spécification publiée : RFC 2652
Applications qui utilisent ce type de support : Ce type de support est le sommet d'une arborescence de types de supports qui expriment des commandes entre les hôtes qui échangent des indices pour les besoins de l'acheminement des référents.
Informations supplémentaires : Ce type de support n'est pas un type autonome. C'est le niveau supérieur d'une arborescence similaire aux arborescences vnd ou prs spécifiées au paragraphe 2.1 de la [RFC2048]. Les types enregistrés au sein de cette arborescence se limitent à des commandes, comme spécifié dans le ou les documents référencés dans la section "Spécification publiée".
Adresse personnelle et de messagerie à contacter pour des informations complémentaires :
Utilisation prévue : UTILISATION LIMITÉE
Auteur/contrôleur des modifications :

Arborescence des réponses

To: ietf-types@iana.org
Subject: Enregistrement du type de support MIME application/index.response

Nom de type de support MIME : application

Nom de sous-type MIME : index.response
Paramètres exigés : code
Paramètres facultatif : aucun
Considérations de codage : aucune
Considérations de sécurité : Les considérations de sécurité entrent en jeu au moins dans les deux scénarios suivants. Il peut y avoir des fuites sur des quantités d'informations d'indexation non désirées sur des éléments confidentiels si elles ne sont pas contrôlées avec soin. À un niveau plus fondamental, le protocole CIP lui-même exige des services externes de sécurité pour fonctionner de manière sûre. Les deux sujets sont traités ci-dessous.
Considérations d'interopérabilité : Les mises en œuvre devraient traiter les commandes inconnues avec douceur.
Spécification publiée : RFC 2652
Applications qui utilisent ce type de support : Ce type de support est utilisé pour coder les réponses aux commandes CIP passées entre des hôtes qui échangent des indices pour les besoins de l'acheminement de référents.
Informations supplémentaires : Ce type de support est un type autonome. Le paramètre code contient le code de réponse spécifique comme spécifié dans l'Appendice B du document de spécification.
Adresse personnelle et de messagerie à contacter pour des informations complémentaires :
Utilisation prévue : UTILISATION LIMITÉE
Auteur/contrôleur des modifications :

Arborescence des objets d'indice

To: ietf-types@iana.org
Subject: Enregistrement du type de support MIME application/index.obj
Nom de type de support MIME : application
Nom de sous-type MIME : index.obj
Paramètres exigés : type, dsi, base-uri
Paramètres facultatif : aucun
Considérations de codage : aucune
Considérations de sécurité : Les considérations de sécurité entrent en jeu au moins dans les deux scénarios suivants. Il peut y avoir des fuites sur des quantités d'informations d'indexation non désirées sur des éléments confidentiels si elles ne sont pas contrôlées avec soin. À un niveau plus fondamental, le protocole CIP lui-même exige des services externes de sécurité pour fonctionner de manière sûre. Les deux sujets sont traités ci-dessous.
Considérations d'interopérabilité : Les mises en œuvre devraient traiter les objets d'indice inconnus conformément aux règles spécifiées dans la spécification publiée.
Spécification publiée : RFC 2652
Applications qui utilisent ce type de support : Ce type de support est le sommet d'une arborescence de types de supports qui expriment les indices qui sont échangés entre des hôtes qui opèrent au sein d'un maillage de référents.
Informations supplémentaires : Ce type de support n'est pas un type autonome. C'est le niveau supérieur d'une arborescence similaire aux arborescences vnd ou prs spécifiées au paragraphe 2.1 de la [RFC2048]. Les types enregistrés au sein de cette arborescence se limitent à des représentations d'indices qui contiennent un résumé des données qui se trouvent dans une base de données et sont utilisées pour générer des référents comme spécifié dans la publication mentionnée ci-dessus.
Adresse personnelle et de messagerie à contacter pour des informations complémentaires :
Utilisation prévue : UTILISATION LIMITÉE
Auteur/contrôleur des modifications :

Arborescence de fabricant

To: ietf-types@iana.org
Subject: Enregistrement du type de support MIME application/index.vnd
Nom de type de support MIME : application
Nom de sous-type MIME : index.vnd
Paramètres exigés : aucun
Paramètres facultatif : aucun
Considérations de codage : aucune
Considérations de sécurité : Les considérations de sécurité entrent en jeu au moins dans les deux scénarios suivants. Il peut y avoir des fuites sur des quantités d'informations d'indexation non désirées sur des éléments confidentiels si elles ne sont pas contrôlées avec soin. À un niveau plus fondamental, le protocole CIP lui-même exige des services externes de sécurité pour fonctionner de manière sûre. Les deux sujets sont traités ci-dessous.
Considérations d'interopérabilité : Les mises en œuvre devraient traiter les objets inconnus avec douceur.
Spécification publiée : RFC 2652
Applications qui utilisent ce type de support : Ce type de support est le sommet d'une arborescence de types de supports qui expriment les extensions spécifiques de fabricant au cadre mentionné dans les spécifications publiées.
Informations supplémentaires : Ce type de support n'est pas un type autonome. C'est le niveau supérieur d'une arborescence similaire aux arborescences vnd ou prs spécifiées au paragraphe 2.1 de la [RFC2048]. Les types enregistrés au sein de cette arborescence se limitent à des extensions spécifiques de fabricant au cadre CIP

comme spécifié dans les publications. Tous les enregistrements au sein de cette arborescence se limitent à ce qui se rapporte aux indices, maillages et référents.

Adresse personnelle et de messagerie à contacter pour des informations complémentaires :
Utilisation prévue : UTILISATION LIMITÉE

Appendice B Codes de réponse

La signification des divers chiffres des codes de réponse est exposée dans la [RFC0821], Appendice E.

Les codes de réponse suivants sont définis pour être utilisés par les serveurs CIPv3. Les mises en œuvre doivent utiliser ces codes exacts ; les codes indéfinis devraient être interprétés par les serveurs CIP comme des erreurs fatales de protocole. Au lieu de définir de nouveaux codes pour des situations non prévues, les mises en œuvre doivent adapter un des codes actuels. La mise en œuvre devrait joindre un autre commentaire utile au code de réponse réutilisé.

Code	**Texte suggéré de description de l'action de l'envoyeur CIP**
220	Message d'annonce de serveur initial.
300	La version de CIP demandée est acceptée. Continuer la transaction CIP dans la version spécifiée.
222	Fermeture de connexion (en réponse à la fermeture de connexion de l'envoyeur). Fin de la transaction.
200	Demande MIME reçue et traitée. On n'attend pas de résultat, continuer (ou fermer) la session.
201	Demande MIME reçue et traitée, le résultat suit. Lire une réponse, délimitée par un délimiteur de message de style SMTP.
400	Temporairement incapable de traiter la demande. Réessayer plus tard. Peut être utilisé pour indiquer que le serveur n'a pas actuellement les ressources disponibles pour accepter un indice.
500	Mauvais format de message MIME. Réessayer avec une demande MIME correctement formatée.
501	Demande inconnue ou manquante dans application/index.cmd. Réessayer avec une commande CIP correcte.
502	Il manque des attributs CIP exigés dans la demande. Réessayer avec des attributs CIP corrects.
520	Interruption de la connexion pour des raisons inattendues. Réessayer et/ou alerter l'administrateur local.
530	La demande exige une signature valide. Signer la demande, si possible, et réessayer. Autrement, faire rapport du problème à l'administrateur.
531	La demande a une signature invalide. Faire rapport du problème à l'administrateur.
532	La signature ne peut être vérifiée. Alerter l'administrateur local, qui devrait coopérer avec l'administrateur distant pour diagnostiquer et résoudre le problème. (Il manque probablement une clé publique.)

5. Déclaration complète de droits de reproduction

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