Groupe de travail Réseau
Request for Comments : 3254
Catégorie : Information

H. Alvestrand, Cisco Systems
avril 2002
Traduction Claude Brière de L'Isle

Définitions pour parler des répertoires

Résumé
Lorsque on discute des systèmes destinés à rendre les informations accessibles sur l'Internet de façon normalisée, il peut être utile que les gens qui en discutent aient une compréhension commune des termes qu'ils utilisent.

Par exemple, une référence au présent document permettrait de s'accorder sur le fait que le système des noms de domaines (DNS, *Domain Name System*) est un répertoire mondial de recherche avec une intégrité de périmètre et une cohérence convergente lâche. D'un autre côté, un serveur de répertoire du protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*) est un répertoire centralisé avec une capacité à la fois de consultation et de recherche.

Le présent document expose un groupe de ces systèmes qui est connu sous le terme de "répertoires".

1. Introduction et termes de base

On suggère d'utiliser les termes suivants pour le reste du document :

- Informations : Faits et idées qui peuvent être représentés (codés) comme données sous des formes variées.

- Données : Informations dans une représentation physique spécifique, usuellement une séquence de symboles qui ont une signification ; en particulier une représentation d'informations qui peuvent être traitées ou produites par un ordinateur. (d'après {RFC2828].)

- Répertoire : Une quantité de données qui sont accessibles par une ou plusieurs méthodes d'accès.

- Demandeur : Entité qui peut (essayer de) accéder aux données d'un répertoire. Noter qu'on ne fait pas d'hypothèse sur la nature du demandeur, animale, végétale, ou minérale.

- Gestionnaire : Entité qui cause les changements des données du répertoire. Généralement, tous les gestionnaires sont des demandeurs, car ils ont aussi besoin de consulter les données, cependant, les rôles sont distincts.

- Méthode d'accès : Une série bien définie d'opérations qui va être cause que les données disponibles d'un répertoire sont obtenues par le demandeur.

- Site : Entité qui héberge tout ou partie d'un répertoire, et le rend disponible par une ou plusieurs méthodes d'accès. Un site peut dans divers contextes être une machine, un centre de données, un réseau de centres de données, ou un seul appareil.

Le présent document n'est pas destiné à être exhaustif ni définitif, mais est destiné à apporter un peu d'aide à la compréhension mutuelle lors de la discussion des méthodes d'accès aux informations à incorporer dans les documents en cours de normalisation de l'Internet.

2. Dimensions de classification

2.1 Unicité et portée

Certains systèmes d'informations sont mondiaux, en ce sens qu'il n'en peut raisonnablement exister qu'un seul dans le monde.

Les autres sont par essence locaux, dans lesquels chaque localité, site ou même boîte va faire tourner son propre magasin d'informations, indépendant de tous les autres.

Les termes suivants sont suggérés :

- Répertoire mondial : répertoire qui ne peut être qu'unique au monde. Le monde lui-même est l'exemple principal ; les allocations de numéros du système téléphonique public selon la Recommandation UIT-T E.164 en sont un autre.

- Répertoire local : classe de répertoires dont plusieurs instances peuvent exister, chacune avec les informations pertinentes pour ce répertoire particulier, sans besoin de coordination entre elles.

- Répertoire centralisé : répertoire où tous les accès aux données doivent passer à travers un seul site.

- Répertoire réparti : répertoire qui n'est pas centralisé ; c'est-à-dire que l'accès aux données peut se faire par plusieurs sites.

- Répertoire dupliqué : répertoire où tous les sites ont les mêmes informations.

- Répertoire coopératif : répertoire réparti où tous les sites n'ont pas toutes les informations, mais où des mécanismes existent pour obtenir les informations pour le demandeur, même lorsque elles ne sont pas disponibles sur le site interrogé à l'origine.

Note: Le terme "mondial" est souvent une affaire de contexte social ou légal ; par exemple, le système E.164 de numérotation téléphonique est mondial par traité international, tandis que le débat sur le point de savoir si le système des noms de domaines est mondial en fait ou juste un répertoire local avec des ambitions s'est révélé le sujet de plus de discussions qu'on ne pourrait énumérer.

Certains disent que la mondialité est dans l'œil du spectateur ; "tout est local dans un certain contexte ". Lorsque on discute de technologie, il peut être avisé d'utiliser plutôt "très largement déployé".

Note: La localisation des répertoires change avec l'échelle de considération. Par exemple, le système mondial du DNS est considéré comme un répertoire coopératif réparti, construit à partir de répertoires de zones qui peuvent eux-mêmes être répartis, et sont toujours dupliqués lorsque répartis.

2.2 Recherche, consultation, interrogation et notification

Quand on décrit les répertoires on doit porter un regard différent sur les types de méthode qu'ils offrent pour trouver les informations.

Les classifications majeures sont :

- Les méthodes de consultation exigent que l'usager connaisse ou devine une valeur exacte avant de demander les informations, qu'on appelle parfois une "clé de consultation" ou "identifiant" et parfois un "nom". Le mot "nom" N'EST PAS recommandé, car il entre en conflit avec d'autres utilisations de ce mot. La réponse à une consultation réussie est un seul groupe d'informations, souvent appelé "informations sur l'entité identifiée". Une méthode de consultation est binaire (oui/non) dans l'accès : elle retourne soit un résultat, soit pas de résultat ; si elle retourne un résultat, c'est le bon résultat pour cette clé de consultation, de sorte que c'est aussi une précision binaire (pas d'information ou une information entièrement pertinente).

- Les méthodes de recherche requièrent de l'usager la connaissance d'une valeur approximative de certaines informations. Elles retourne usuellement zéro, une, ou plusieurs réponses qui correspondent aux informations fournies selon un certain algorithme. Lorsque le répertoire est structuré autour "d'entités", les informations peuvent être sur zéro, une, ou de nombreuses entités.

En termes de base de données, une méthode de consultation s'apparente à une interrogation correspondant exactement à une clé unique sur un tableau ; toutes les autres interrogations de la base de données devraient être classées comme méthodes de "recherche".

En général, les répertoires qui offrent des méthodes de recherche plus souples peuvent aussi laisser de la place pour des interrogations ad hoc, des précisions sur une interrogation antérieure, une correspondance approximative et d'autres aides ; cela peut conduire à de nombreuses combinaisons différentes de précision et d'accès.

On peut définir les termes pour énumérer ce qu'on obtient de ces répertoires :

Précision est le degré auquel ce qu'on a demandé est ce qu'on veut (pas d'information étrangère).

Accès est la capacité à s'assurer que toutes les données pertinentes du répertoire sont retournées.

Des erreurs de type I surviennent lorsque les données pertinentes existent dans le répertoire, mais ne sont pas retournées.

Des erreurs de type II surviennent lorsque des données non pertinentes sont retournées dans un résultat d'interrogation.

Noter que ces concepts ne peuvent être appliqués que lorsque la "pertinence" de la propriété est bien définie ; c'est-à-dire, si elle dépend de ce à quoi le répertoire est utilisé. On trouvera un développement de cette discussion dans [KORFHAGE].

Une autre dimension de ces question est celle du temps :

- Les répertoires d'interrogation vont répondre à une demande par une réponse, et une fois que c'est fait, ne vont rien faire de plus.

- Les répertoires de notification vont avoir une demande de la part d'un usager pour des informations qui seront retournées ultérieurement lorsque elles seront disponibles, actuelles, ou autre, et le répertoire va répondre à ce moment là en notifiant à l'usager que les informations sont disponibles.

- Les répertoires d'abonnement sont comme les répertoires de notification, mais vont transférer les informations réelles lorsqu'elles sont disponibles.

2.3 Modèles de cohérence

La cohérence (ou son absence) est une propriété des répertoires répartis ; pour les besoins de cet exposé, on ignorera la question des données sémantiquement incohérentes (comme l'occurrence d'une grossesse chez un homme) et on se concentrera sur le problème de la cohérence lorsque l'incohérence est définie comme faisant la même demande, en utilisant les mêmes accréditifs, on a en réponse des données différentes sur des sites différents.

Les répertoires répartis peuvent être ;

- En cohérence stricte, où le problème ci-dessus ne se pose jamais. C'est assez difficile ; les répertoires qui offrent cette propriété sont généralement assez contraignants et/ou assez coûteux.

- En cohérence interne stricte, où les réponses reflètent toujours un tableau cohérent du répertoire total, mais certains sites peuvent refléter une version du répertoire plus ancienne que celle des autres.

- En cohérence lâche, convergente, où des parties différentes du répertoire peuvent être mises à jour à des moments différents si on le voit à partir d'un seul site, mais le processus est conçu de telle sorte que si on arrête de faire les changements au répertoire, tous les sites vont tôt ou tard présenter les mêmes informations.

- Incohérents, où aucune garantie ne peut jamais être donnée.

Une variante intéressante est la cohérence de sous ensembles, où le système est cohérent (selon une des définitions ci-dessus) mais où il ne sera pas répondu à toutes les questions sur tous les sites ; éventuellement parce que des sites différents ont des politiques différentes sur ce qu'ils mettent à disposition (NetNews) ou parce que des sites différents ont seulement besoin de sous ensembles différents du "tableau complet" (BGP).

2.4 Modèles de sécurité

Il est plus difficile de décrire les modèles de sécurité en quelques phrases que les autres propriétés des systèmes d'informations. Il existe aussi une abondante littérature spécialisée sur la terminologie de la sécurité, dont la {RFC2828].

Voici cependant quelques réflexions :

Sur la confiance dans les données : pourquoi croit on que des données sont correctes ?

- parce que elles sont dans le répertoire (et donc qu'elles ont dû avoir été autorisées). C'est le périmètre (ou coquille d'œuf) d'intégrité.

- parce qu'il contient des vérifications d'intégrité internes, qui impliquent usuellement des signatures numériques par des identités vérifiables. C'est l'intégrité des éléments ; la granularité de l'intégrité et la capacité à faire des vérifications d'intégrité sur les relations entre les objets est extrêmement importante et extrêmement difficile à faire correctement, comme l'est d'établir les racines de la chaîne de confiance.

- parce que cela est cohérent avec des informations disponibles, et fait que les choses appropriées se passent quand on les utilise. C'est l'intégrité souhaitée.

Le choix du modèle d'intégrité est une affaire d'évaluation du coût de mise en œuvre de l'intégrité (coût), de la valeur qu'on accorde à l'intégrité de la ressource protégée (valeur) et de l'impact du coût sur les affaires (risque).

Sur l'accès aux informations, les catégories usuelles s'appliquent :

- Accès ouvert : tout le monde peut accéder aux informations.

- Accès foncé sur une propriété : l'accès dépend de qui vous êtes, où de l'endroit où vous êtes. Par exemple, limité au "même réseau", "physiquement présent", ou "nom DNS résoluble".

- Accès fondé sur l'identité : on a accès parce qu'on est (ou qu'on réussi à se faire passer pour) une certaine personne. (C'est-à-dire, nom d'utilisateur/mot de passe, certificats personnels ou autres informations vérifiables.) Ceci s'appuie sur une couche qui spécifie ce à quoi l'identité qui a été prouvée a accès.

- Accès fondé sur un jeton : on a accès à cause de ce qu'on a. Jetons matériels, cartes à mémoire, certificats, ou clés de capacité. Dans ce cas, l'accès est donné à tous ceux qui peuvent présenter cet accréditif, sans se soucier de leur identité.

Les approches les plus courantes sont celles fondées sur l'identité et l'accès ouvert ; cependant, l'accès par "ce qu'on a" est couramment utilisé de façon informelle dans, par exemple, FTP protégé par mot de passe ou les sites de la Toile où le mot de passe est partagé entre tous les membres d'un groupe.

2.5 Modèles de mise à jour

Quelques exemples :

- Les répertoires en lecture seule n'ont pas de moyens standard pour changer leurs informations. Cela se fait habituellement par une autre interface que l'interface standard.

- Les répertoires principalement en lecture sont conçus sur la base de la théorie selon laquelle la lecture est bien plus fréquente que les mises à jour ; cela peut, par exemple, être reflété dans des protocoles de mise à jour de cohérence relativement lents.

- Les répertoires en lecture écriture supposent que les mises à jour et les opérations de lecture sont du même ordre de grandeur.

- Les répertoires principalement en écriture sont conçus pour mémoriser un flux de données entrant, et lorsque il est nécessaire de reproduire des éléments de données pertinentes du flux. Des exemples typiques sont des bases de données de compagnie d'assurance et des journaux d'audit.

2.6 Le terme "répertoire"

Les définitions ci-dessus n'ont jamais utilisé le terme "Annuaire".

Dans les usages les plus courants, les propriétés que doit avoir un répertoire afin qu'il vaille la peine de l'appeler un annuaire sont :

- recherche

- Cohérence convergente

Tous les autres termes ci-dessus peuvent varier à travers l'ensemble des choses qui sont appelées des "annuaires".

3. Classification de quelques systèmes réels

3.1 Le système des noms de domaines

Le DNS [RFC1034] est un répertoire mondial coopératif de consultation avec une cohérence convergente lâche et seulement une capacité d'interrogation.

Il est soit strictement en lecture seule, soit principalement en lecture (avec le DNS dynamique) ; il a un modèle d'accès ouvert, et principalement une intégrité de périmètre (certains diraient une intégrité souhaitée). DNSSEC {RFC2535] vise à lui donner l'intégrité des éléments.

Le DNS est construit sur des répertoires de zones qui eux-mêmes peuvent être répartis, et sont toujours dupliqués lorsque ils sont répartis.

Noter que comme beaucoup d'autres systèmes, le DNS a des caractéristiques qui ne rentrent pas nettement dans la classification ; par exemple, il y a une fonction (déconseillée et pas très utilisée) appelée IQUERY, qui admet une capacité très limitée d'interrogation.

Si on ouvre la boîte et qu'on regarde les relations entre les serveurs de noms primaires et secondaires, cela peut être vu comme une forme limitée de capacité de notification, mais ce n'est pas disponible à l'utilisateur final du système total.

3.2 Le répertoire mondial X.500 (imaginaire)

X.500 {RFC1308] était destiné à être un répertoire mondial de recherches avec une cohérence convergente lâche.

Il était destiné à être principalement en lecture, à périmètre sécurisé et capable d'interrogation.

3.3 La base de données mondiales d'informations d'acheminement de BGP

La base de données d'informations d'acheminement mondial ou de niveau supérieur de BGP [BGP1] est souvent vue comme un répertoire mondial en lecture écriture avec une cohérence de sous ensemble convergente lâche (tous les chemins ne sont pas portés partout) et un contrôle d'intégrité très limité, principalement destiné à être fondé sur l'intégrité de périmètre, avec un "contrôle d'accès fondé sur ce que vous êtes".

On peut objecter que BGP {RFC1771] est plutôt un mécanisme mondial pour mettre à jour un ensemble de répertoires locaux en lecture/écriture, car on est loin d'avoir toutes les informations d'acheminement apportées partout, et la décision sur quel chemin accepter est toujours considérée une affaire de politique locale. Mais du point de vue du modèle de sécurité, une grande partie des contrôles est appliquée à la périphérie du système d'acheminement, et non dans chaque répertoire local ; cela rend quand même intéressant de considérer les propriétés qui s'appliquent au système BGP comme un tout.

3.4 Le système NetNews

NetNews {RFC0977] est un répertoire mondial en lecture écriture avec une cohérence de sous ensembles lâche (non convergente) (tous les sites ne portent pas tous les articles, et la durée de rétention des article diffère). Entre les sites, il offre des capacités d'abonnement ; aux usagers, il offre des fonctions à la fois de recherche et de consultation.

3.5 Les MIB de SNMP

Un agent SNMP [{RFC2570] peut être vu comme un répertoire local, centralisé, offrant une fonction de consultation.

Avec SNMPv3, il offre toutes sortes de modèles d'accès, mais principalement, un "accès à cause de ce que vous avez", semble populaire.

4. Considérations pour la sécurité

La sécurité est une question très pertinente lorsque on parle des systèmes d'accès à l'information.

Les questions à considérer sont :
- l'accès contrôlé aux informations,
- le contrôle des droits à mettre à jour les informations,
- la protection du chemin des informations entre fournisseur et consommateur,
- la question de la confidentialité des informations personnelles,
- les interactions entre plusieurs façons d'accéder aux mêmes informations.

C'est probablement une bonne chose de considérer avec attention les modèles de sécurité du paragraphe 2.4 lors de la conception de répertoires ou de protocoles d'accès à des répertoires.

5. Remerciements

L'auteur souhaite remercier tous ceux qui ont contribué au présent document, parmi lesquels Patrik Faltstrom, Eric A. Hall, James Benedict, Ted Hardie, Urs Eppenberger, John Klensin, et de nombreux autres.

6. Références

[BGP1] "Analyzing the Internet's BGP Routing Table", publié dans le "The Internet Protocol Journal", Volume 4, n° 1, avril 2001. Disponible à http://www.telstra.net/gih/papers/ipj/4-1-bgp.pdf

[E164] Recommandation UIT-T E.164/I.331 "Plan de numérotage des télécommunications publiques internationales". (05/97).

[KORFHAGE] Robert R. Korfhage, "Information Storage and Retrieval", Wiley 1997. Voir à la page 194 la définition de "precision" et de "recall".

[RFC0977] B. Kantor et P. Lapsley, "Protocole de transfert des nouvelles du réseau", février 1986. *(Obsolète, voir* RFC3977)

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987.

[RFC1308] C. Weider et J. Reynolds, "Introduction applicative aux services d'annuaire utilisant le protocole X.500", FYI0013, mars 1992. *(Information)*

[RFC1771] Y. Rekhter, T. Li , "Protocole de routeur frontière v. 4 (BGP-4)", mars 1995. *(Obsolète, voir* RFC4271) *(D.S.)*

[RFC2535] D. Eastlake, 3rd, "Extensions de sécurité du système des noms de domaines", mars 1999. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

[RFC2570] J. Case, R. Mundy, D. Partain, B. Stewart, "Introduction à la version 3 du cadre de gestion de réseau de l'Internet", avril 1999. (*Obsolète, voir* RFC3410) *(Information)*

[RFC2828] R. Shirey, "Glossaire de la sécurité sur l'Internet", FYI 36, mai 2000. (*Obsolète, voir* RFC4949)

7. Adresse de l'auteur

Harald Tveit Alvestrand
Cisco Systems
Weidemanns vei 27
N-7043 Trondheim
NORWAY

téléphone : +47 41 44 29 94
mél : Harald@alvestrand.no

8. Déclaration complète de droits de reproduction

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