Groupe de travail Réseau
**Request for Comments : 4018**
Catégorie : En cours de normalisation

Traduction Claude Brière de L'Isle

M. Bakke, Cisco
J. Hufferd & K. Voruganti, IBM
M. Krueger, HP
T. Sperry, Adaptec
avril 2005

# Découverte de cibles et des serveurs de noms des interfaces systèmes de petits ordinateurs (iSCSI) en utilisant le protocole de localisation de service version 2 (SLPv2)



**Résumé**
Le protocole iSCSI donne aux hôtes un moyen pour accéder aux appareils SCSI sur un réseau IP. Le présent document définit l'utilisation du protocole de localisation de service (SLP, *Service Location Protocol*) par les hôtes, appareils et services de gestion iSCSI, ainsi que les gabarits de type de service SLP qui décrivent les services qu'ils fournissent.

## des Matières



## 1. Introduction

iSCSI [RFC3720] est un protocole utilisé pour transporter les commandes, données, et états SCSI [SAM2] à travers un réseau IP. Le présent protocole est en mode connexion et est actuellement défini sur TCP. iSCSI utilise une relation client-serveur. L'extrémité client de la connexion est un initiateur, et il envoie des commandes SCSI ; l'extrémité serveur de la connexion est appelée la cible, et reçoit et exécute les commandes.

Les initiateurs iSCSI peuvent utiliser plusieurs méthodes pour trouver les cibles auxquelles ils veulent se connecter. Deux de ces méthodes peuvent être réalisées sans l'aide de SLP :
- Chaque cible et son adresse peuvent être configurées statiquement sur l'initiateur.

- Chaque adresse qui fournit des cibles peut être configurée sur l'initiateur ; iSCSI fournit un mécanisme par lequel l'initiateur peut interroger l'adresse sur une liste de cibles.

Les méthodes ci-dessus sont définies plus en détails dans la [RFC3721] "Interface Internet des systèmes de petits ordinateurs (iSCSI) : dénomination et découverte".

Chacune des méthodes ci-dessus exige qu'une petite quantité de configuration soit faite sur chaque initiateur. La capacité à découvrir les cibles et les services de noms sans avoir à configurer les initiateurs est une caractéristique désirable. Le protocole de localisation de service (SLP, *Service Location Protocol*) [RFC2608] est un protocole sur la voie de la normalisation de l'IETF fournissant plusieurs caractéristiques qui vont simplifier la localisation des services iSCSI. Le présent document décrit comment SLP peut être utilisé dans des environnements iSCSI pour découvrir des cibles, des adresses qui fournissent des cibles, et des serveurs de gestion de mémorisation.

## 2. Conventions de notation

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].

## 3. Terminologie

Voici quelques définitions qui peuvent aider les lecteurs qui ne sont pas familiarisés avec SLP, SCSI, ou iSCSI. Certaines de ces définitions ont été reproduites de la [RFC2608] et de "Trouver un serveur RSIP avec SLP" [RFC3105].

Agent d'utilisateur (UA, *User Agent*) : processus qui fonctionne au nom du client pour établir le contact avec un certain service. L'UA restitue les informations de service à partir des agents de service ou des agents de répertoire.

Agent de service (SA, *Service Agent*) : processus qui fonctionne au nom d'un ou plusieurs services pour annoncer les services et leurs capacités.

Agent de répertoire (DA, *Directory Agent*) : processus qui collecte les annonces de service. Il ne peut y avoir qu'un seul DA pour chaque hôte.

Portée : ensemble désigné de services, constituant normalement un groupe administratif logique.

Annonce de service : un URL, des attributs, et une durée de vie (qui indique combien de temps l'annonce est valide) qui fournissent des informations d'accès aux services et une description des capacités d'un service particulier.

Initiateur : entité logique, normalement au sein d'un hôte, qui envoie des commandes SCSI aux cibles pour qu'elles soient exécutées. Un initiateur est généralement présent sous la forme d'un pilote d'appareil.

Cible : entité logique, normalement au sein d'un contrôleur de mémorisation ou d'une passerelle qui reçoit des commandes SCSI d'un initiateur et les exécute. Une cible inclut une ou plusieurs unités logiques (LU, *Logical Unit*) ; chaque LU est un appareil SCSI, comme un disque ou un lecteur de bandes.

Nom iSCSI : chaîne de caractères UTF-8 qui sert d'identifiant unique pour les initiateurs et cibles iSCSI. Son format et son usage sont précisés dans la [RFC3721].

Client iSCSI : entité logique, normalement un hôte qui comporte au moins un initiateur iSCSI.

Serveur iSCSI : entité logique, normalement un contrôleur de mémorisation ou une passerelle qui comporte au moins une cible iSCSI.

Serveur de gestion de mémorisation : entité adressable qui fournit des services de gestion dont profite un environnement iSCSI. "Serveur de gestion de mémorisation" est utilisé comme terme générique et n'indique pas un protocole ou service spécifique.

# 4. Utilisation de SLP pour la découverte de service iSCSI

Deux entités sont impliquées dans la découverte iSCSI. Le résultat final est qu'un initiateur iSCSI (par exemple, un hôte) découvre les cibles iSCSI, généralement fournies par des contrôleurs de mémorisation ou des passerelles.

Les cibles iSCSI sont enregistrées par SLP comme un ensemble d'URL de service, un pour chaque adresse sur laquelle la cible peut être jointe. Les initiateurs découvrent ces cibles en utilisant les demandes de service SLP. Les cibles qui ne prennent pas directement en charge SLP ou qui sont sous le contrôle d'un service de gestion peuvent être enregistrées par un agent de service mandataire au titre du logiciel qui fournit ce service.

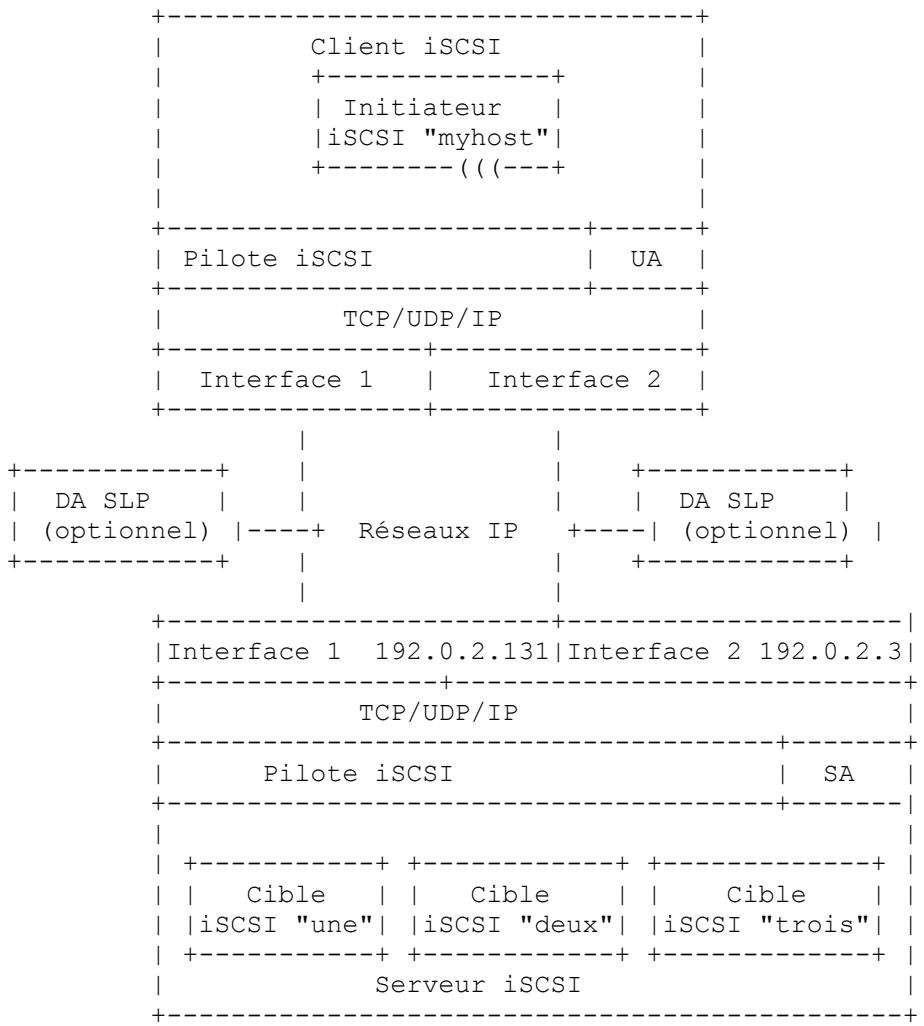
Les entités iSCSI peuvent aussi utiliser SLP pour découvrir des services de gestion de niveau supérieur lorsque ceux-ci sont nécessaires.

Cette section décrit d'abord l'utilisation de SLP pour la découverte des cibles par les initiateurs iSCSI, puis elle décrit l'utilisation de SLP pour découvrir les serveurs de gestion de mémorisation.

Le présent document suppose que SLPv2 sera utilisé pour découvrir les services en rapport avec iSCSI ; on ne tente pas d'y inclure la prise en charge de SLPv1.

## 4.1 Découverte de cibles iSCSI avec SLP

Le diagramme qui suit montre les relations entre les clients, serveurs, initiateurs, et cibles iSCSI. Un client iSCSI inclut au moins un initiateur iSCSI, et un agent d'utilisateur (UA, *user agent*) SLP. Un serveur iSCSI inclut au moins une cible iSCSI et un agent de service (SA, *service agent*) SLP. Certaines entités, comme des moteurs de copie étendus, incluent des initiateurs et des cibles. Elles incluent un SA, pour que ses cibles soient découvertes, et un UA, pour que ses initiateurs découvrent les autres cibles.



Dans le dessin ci-dessus, le serveur iSCSI a trois cibles iSCSI que le client pourrait découvrir, appelées "une", "deux" et "trois". Le client iSCSI a un initiateur iSCSI du nom de "myhost". Le client iSCSI peut utiliser le nom de l'initiateur dans ses demandes de service SLP comme un filtre pour découvrir seulement les cibles qui sont configurées à accepter des connexions iSCSI provenant de "myhost".

Chaque cible et initiateur iSCSI a un nom unique, appelé un nom iSCSI. Cet identifiant est le même sans considération du chemin réseau (à travers des cartes d'adaptateur, des réseaux, et des interfaces sur l'appareil de mémorisation) sur lequel la cible est découverte et accédée. Pour cet exemple, les noms iSCSI "une", "deux", et "trois" sont utilisés pour les cibles ; l'initiateur utilise le nom "myhost". Un nom iSCSI réel incorporerait plus de structures, incluant une autorité de désignation, et ne sont pas décrites ici.

Chacune des cibles iSCSI dans le dessin peut apparaître à deux adresses, car deux interfaces réseau sont présentes. Chaque cible aurait deux URL de service, sauf si un seul URL de service inclut un nom d'hôte DNS se transposant dans les deux adresses.

Un URL de cible iSCSI consiste en son nom d'hôte pleinement qualifié ou son adresse IP, l'accès TCP sur lequel il écoute, et son nom iSCSI. Un serveur iSCSI doit enregistrer chacune de ses cibles individuelles à chacune de ses adresses réseau.

Le serveur iSCSI construit une annonce de service du type "service:iscsi:cible" pour chacun des URL de service qu'il souhaite enregistrer. L'annonce contient une durée de vie, ainsi que d'autres attributs qui sont définis dans le gabarit de service.

Si le serveur dans le dessin ci-dessus écoute à l'accès TCP 3260 pour les deux adresses réseau, l'URL de service enregistré serait :
- 192.0.2.131:3260/une
- 192.0.2.131:3260/deux
- 192.0.2.131:3260/trois
- 192.0.2.3:3260/une
- 192.0.2.3:3260/deux
- 192.0.2.3:3260/trois

Le reste de la procédure de découverte est identique à celle utilisée par toute paire client/serveur qui met en œuvre SLP :
1. Si un DA SLP est trouvé, le SA contacte le DA et enregistre l'annonce de service. Que un ou plusieurs DA SLPv2 soient ou non découverts, le SA conserve l'annonce elle-même et répond directement aux interrogations d'UA en diffusion groupée.
2. Lorsque l'initiateur iSCSI demande des informations de contact pour une cible iSCSI, l'UA contacte le DA en utilisant l'envoi individuel ou le SA en utilisant la diffusion groupée. Si un UA est configuré avec l'adresse du SA, il peut éviter d'utiliser la diffusion groupée et peut contacter un SA en utilisant l'envoi individuel. L'UA inclut une interrogation sur la base des attributs pour indiquer les caractéristiques de la ou des cibles qu'il demande.
3. Une fois que l'UA a le nom de l'hôte ou l'adresse du serveur iSCSI, ainsi que le numéro d'accès et le nom de la cible iSCSI, il peut commencer la connexion iSCSI normale à la cible.

Comme les informations contenues dans le gabarit de cible iSCSI peuvent excéder les tailles courantes de datagramme réseau, la mise en œuvre de SLP pour les UA et les SA qui prennent en charge ce gabarit DOIT mettre en œuvre SLP sur TCP.

### 4.1.1 Trouver des cibles sur la base des accréditifs d'initiateur

Pour que lui soit permis l'accès à une cible iSCSI, un initiateur doit être authentifié. L'initiateur peut être obligé par la cible de produire un ou plusieurs des accréditifs suivants :
- un nom d'initiateur iSCSI,
- une adresse IP,
- un accréditif CHAP, SRP, ou Kerberos,
- toute combinaison des précédents.

La plupart des cibles iSCSI ne permettent l'accès qu'à un ou deux initiateurs. Dans le scénario idéal de découverte, un initiateur va envoyer une demande SLP et recevoir des réponses SEULEMENT pour les cibles auxquelles l'initiateur a la garantie d'une connexion réussie. Pour y arriver, le gabarit de cible iSCSI contient les attributs suivants, dont chacun admet une liste de valeurs :
1. auth-name : cet attribut contient la liste des noms d'initiateur auxquels l'accès à cette cible est permis, ou la valeur "any", qui indique qu'aucun nom d'initiateur spécifique n'est exigé.
2. auth-addr : cet attribut contient la liste des nom d'hôtes et/ou d'adresses IP à qui l'accès à la cible sera permis, ou la

valeur "any", qui indique qu'aucune adresse ou nom d'hôte spécifique n'est exigé. Si un grand nombre d'adresses est permis (peut-être un sous réseau) cet attribut peut contenir la valeur "any".

3. auth-cred : cet attribut contient une liste d'accréditifs de "méthode/identifiant" à qui seront permis l'accès à la cible, pourvu qu'ils puissent produire le mot de passe correct ou un autre vérificateur durant le processus de connexion. Si aucun accréditif spécifique n'est exigé, la valeur "any" est utilisée.

La liste des chaînes de méthodes valides pour auth-cred est définie dans la [RFC3720], paragraphe 11.1, "AuthMethod". L'identifiant utilisé après le "/" est défini par le AuthMethod spécifique, aussi dans la [RFC3720]. Des exemples montrant les recherches de l'initiateur sur la base des attributs auth-xxxx sont montrés dans la section spécifique du gabarit de cible spécifique ci-dessous.

Noter aussi que les attributs auth-xxxx sont considérés comme des informations de politique de sécurité. Si ces attributs sont répartis, IPsec DOIT être mis en œuvre comme spécifié au paragraphe 6.1 "Mise en œuvre de la sécurité".

### 4.1.2 Prise en charge de l'accès à la même cible par plusieurs identités

Si une cible veut permettre l'accès à plusieurs identités d'hôte, plus d'une combinaison d'attributs auth-xxxx devront être permises. Dans certains de ces cas, il n'est pas possible d'exprimer tout l'ensemble des combinaisons valides d'attributs auth-xxxx dans un seul enregistrement d'URL de service. Par exemple, si on peut s'adresser à une cible avec :

auth-name=myhost1 ET auth-cred=CHAP/usager1 (identité1)

OU

auth-name-myhost2 ET auth-cred=CHAP/usager2 (identité2)

ce qui est ci-dessus ne peut être spécifié dans un seul enregistrement d'URL de service, car (auth-name=myhost1, auth-name=myhost2, auth-cred=CHAP/usager1, auth-cred=CHAP/usager2) permettrait d'utiliser tout auth-name avec tout auth-cred. Cela rend nécessaire la capacité d'enregistrer une cible et une adresse sous plus d'un URL de service, une pour (identité1) et une pour (identité2).

Parce que l'URL de service doit être unique, (identité1) et (identité2) doivent chacune être enregistrées sous un URL de service unique. Pour les systèmes qui prennent en charge la configuration d'identités multiples pour accéder à une cible, l'URL de service doit contenir une chaîne opaque supplémentaire qui définit l'identité. Cela apparaît après le nom iSCSI dans la chaîne d'URL et est séparé par un caractère "/". Chaque triplet enregistré (cible-adresse, cible-nom, initiateur-identité) peut alors enregistrer un ensemble d'attributs auth-xxxx.

### 4.1.3 Utilisation de SLP dans un environnement qui n'est pas de diffusion groupée

Dans certains réseaux, l'utilisation de la diffusion groupée pour les besoins de la découverte est soit indisponible, soit interdite. Cela inclut des réseaux publics ou de fournisseur de service qui sont placés entre un client et un serveur iSCSI. Il sont probablement plus courants entre deux passerelles iSCSI, une sur un site de fournisseur de service de mémorisation, et l'autre sur un site de consommateur.

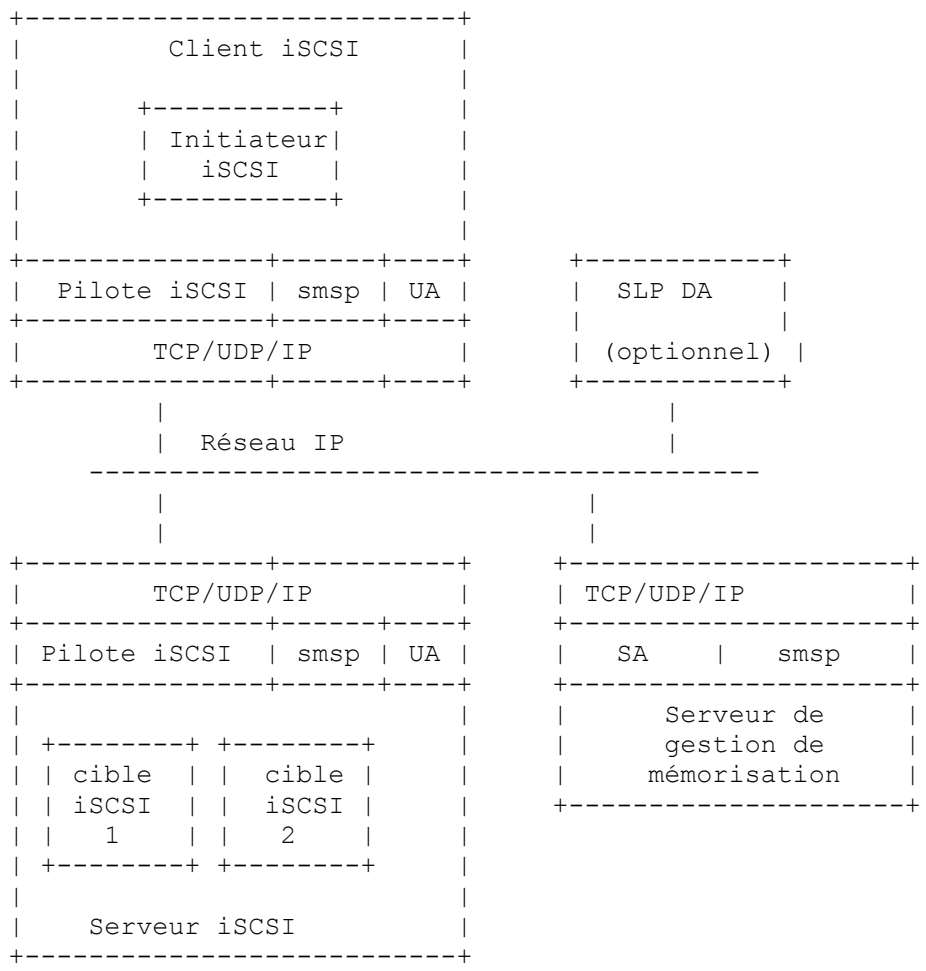
Dans ces réseaux, un initiateur peut permettre la configuration des adresses d'un ou plusieurs SA au lieu de, ou en plus de sa configuration de DA. L'initiateur va alors faire les demandes de service SLP en envoi individuel directement à ces SA, sans utiliser d'abord la diffusion groupée pour les découvrir.

Cette fonctionnalité est tout à fait dans le domaine d'application du présent protocole SLP. La principale conséquence pour les mises en œuvre est qu'un initiateur configuré à faire des demandes directes en envoi individuel à un SA devra ajouter cela à l'API SLP, si il suit l'API de localisation de service définie dans la [RFC2614].

## 4.2 Découverte de services de gestion de mémorisation avec SLP

Les serveurs de gestion de mémorisation peuvent être construits pour gérer et contrôler l'accès aux cibles de différentes façons. Ils peuvent fournir de nombreux services au delà de la découverte, qui pourraient inclure l'allocation et la gestion de mémorisation. Aucun de ces services n'est défini ici; l'intention du présent document est de permettre que ces services soient découverts par les clients et les serveurs, en plus de la découverte de la cible qui est déjà effectuée aujourd'hui.

Le dessin qui suit montre un client iSCSI, un serveur iSCSI, et un serveur de gestion de mémorisation. Pour simplifier le dessin, le second réseau IP n'est pas montré mais on suppose qu'il existe. Le serveur de gestion de mémorisation utiliserait son propre protocole (smsp) pour fournir des capacités aux clients et serveurs iSCSI ; ces clients et serveurs peuvent utiliser SLP pour découvrir le serveur de gestion de mémorisation.




Note r la différence entre le modèle de serveur de gestion de mémorisation et le modèle précédemment défini de découverte de cible. Lorsque la découverte de cible était utilisée, le serveur iSCSI mettait en œuvre un SA, à découvrir par l'UA de l'initiateur. Dans le modèle de serveur de gestion de mémorisation, le client et les serveurs iSCSI mettent tous en œuvre des UA, et le serveur de gestion met en œuvre le SA.

Un URL de serveur de gestion de mémorisation contient le nom de domaine ou l'adresse IP et le numéro d'accès TCP ou UDP. Aucune autre information n'est requise.

Le serveur de gestion de mémorisation construit une annonce de service du type "service:iscsi:sms" pour chacune des adresses auxquelles il apparaît. L'annonce contient l'URL et une durée de vie, ainsi que d'autres attributs qui sont définis dans le gabarit de service.

Le reste de la procédure de découverte est identique à celle utilisée pour découvrir les cibles iSCSI, sauf que les initiateurs et les cibles seraient normalement des "clients" du service de gestion de mémorisation.

Les cibles qui prennent en charge un service de gestion de mémorisation mettent en œuvre un UA en plus du SA. Une cible peut autrement juste mettre en œuvre l'UA et permettre au service de gestion de mémorisation d'annoncer ses cibles de façon appropriée en fournissant un SA et en enregistrant les enregistrements appropriés de service:iscsi:cible au nom de la cible: L'appareil cible n'aura pas à annoncer ses propres cibles. Ceci n'a pas d'impact sur l'initiateur.

Ceci permet à la découverte des cibles de l'initiateur d'être complètement interopérable sans considération du service de gestion de mémorisation qui est utilisé, qu'il ne soit pas utilisé du tout, ou que les enregistrement de cibles soient fournis directement par la cible ou par le service de gestion.

### 4.3 Considérations d'internationalisation

SLP permet que des chaînes internationalisées soient enregistrées et restituées. Les attributs dans le gabarit qui ne sont pas marqués avec un 'L' (littéral) seront enregistrés d'une manière localisée. Une localisation "en" (English) DOIT être enregistrée, et d'autres PEUVENT être enregistrées.

Les attributs qui incluent des caractères non ASCII seront codés en utilisant UTF-8, comme décrit dans les [RFC3722] et [RFC3491].

## 5. Gabarits SLP pour iSCSI

Trois gabarits sont fournis : un gabarit de cible iSCSI, un gabarit de service de gestion, et un gabarit abstrait pour encapsuler les deux.

### 5.1 Gabarit de type de service abstrait iSCSI

Ce gabarit définit le service abstrait "service:iscsi". Il est utilisé comme service de niveau supérieur pour encapsuler tous les autres services en rapport avec iSCSI.

Nom du soumettant : Mark Bakke
Langage du gabarit de service : en
Considérations de sécurité : voir la Section 6.

Texte du gabarit :
----------le gabarit commence ici----------
template-type=iscsi
template-version=1.0

template-description=
Ceci est un type de service abstrait. L'objet du type de service iscsi est d'englober tous les services utilisés en soutien du protocole iSCSI.

template-url-syntax=
  url-path= ; Dépend du type de service concret.

----------le gabarit se termine ici----------

### 5.2 Gabarit de type de service concret de cible iSCSI

Ce gabarit définit le service "service:iscsi:cible". Une entité qui contient des cibles iSCSI qui souhaitent être découvertes via SLP va enregistrer chacune d'elles, avec leurs adresses, comme de type de service.

Les initiateurs (et peut-être les services de gestion) qui souhaitent découvrir des cibles de cette façon vont généralement utiliser une des interrogations suivantes :

1. Trouver une cible spécifique, connaissant son nom de cible iSCSI :
Service : service:iscsi:cible
Portée : initiator-scope-list
Interrogation : (iscsi-name=iqn.2001-04.com.exemple:sn.456)

2. Trouver tous les noms de cibles iSCSI qui peuvent permettre l'accès à un certain initiateur :
Service : service:iscsi:cible
Portée : initiator-scope-list
Interrogation : (auth-name=iqn.1998-03.com.exemple:hostid.045A7B)

3. Trouver tous les noms de cibles iSCSI qui peuvent permettre l'accès de tout initiateur :
Service : service:iscsi:cible
Portée : initiator-scope-list
Interrogation : (auth-name=any)

4. Trouver tous les noms de cibles iSCSI qui peuvent permettre l'accès à cet initiateur, ou qui vont permettre l'accès à tout initiateur :
Service: service:iscsi:cible
Portée : initiator-scope-list
Interrogation : &(auth-name=iqn.1998-03.com.exemple:hostid.045A7B) (auth-name=any)

5. Trouver tous les noms de cibles iSCSI qui peuvent permettre l'accès à un certain nom d'utilisateur CHAP :
Service : service:iscsi:cible
Portée : initiator-scope-list
Interrogation : (auth-cred=chap/my-user-name)

6. Trouver tous les noms de cibles iSCSI qui peuvent permettre l'accès à un certain initiateur qui prend en charge deux adresses IP, un accréditif CHAP et un accréditif SRP, et un nom d'initiateur :
Service : service:iscsi:cible
Portée : initiator-scope-list
Interrogation : &(|(auth-name=iqn.com.exemple:host47)(auth-name=any)
|(auth-addr=192.0.2.3)(auth-addr=192.0.2.131)(auth-addr=any)
|(auth-cred=chap/foo)(auth-cred=srp/my-user-name)(auth-cred=any))

7. Trouver les noms de cibles iSCSI à partir desquelles un certain initiateur à la permission de se connecter :
Service : service:iscsi:cible
Portée : initiator-scope-list
Interrogation : (boot-list=iqn.1998-03.com.exemple:hostid.045A7B)

8. De plus, un service de gestion peut souhaiter découvrir toutes les cibles :
Service : service:iscsi:cible
Portée : management-server-scope-list
Interrogation : <chaîne-vide>

Plus de détails sur l'amorçage à partir d'une cible iSCSI sont donnés dans la [RFC4173].

Nom du soumettant : Mark Bakke
Langage du gabarit de service : en
Considérations de sécurité : voir la Section 6.

Texte du gabarit
----------le gabarit commence ici----------
template-type=iscsi:cible
template-version=1.0

template-description=
C'est un type de service concret. Le type de service iscsi:cible est utilisé pour enregistrer des adresses de cibles individuelles à découvrir par d'autres. Les UA vont généralement les chercher en incluant un des éléments suivants :
- le nom de cible iSCSI,
- les identifiants d'initiateur iSCSI (nom iSCSI, accréditif, adresse IP),
- l'URL de service.

template-url-syntax=
```
url-path    = hostport "/" iscsi-name [ "/" identity ]
hostport    = host [ ":" port ]
host        = hostname / hostnumber  ; nom DNS ou adresse IP
hostname    = *( domainlabel "." ) toplabel
alphanum    = ALPHA / DIGIT
domainlabel = alphanum / alphanum *[alphanum / "-"] alphanum
toplabel    = ALPHA / ALPHA *[ alphanum / "-" ] alphanum
hostnumber  = ipv4-number / ipv6-addr  ; adresse IPv4 ou IPv6
ipv4-number = 1*3DIGIT 3("." 1*3DIGIT)
ipv6-addr   = "[" ipv6-number "]"
ipv6-number =  6( h16 ":" ) ls32 / "::" 5( h16 ":" ) ls32 / [ h16 ] "::" 4( h16 ":" ) ls32
            / [ *1( h16 ":" ) h16 ] "::" 3( h16 ":" ) ls32 / [ *2( h16 ":" ) h16 ] "::" 2( h16 ":" ) ls32
            / [ *3( h16 ":" ) h16 ] "::"  h16 ":"   ls32 / [ *4( h16 ":" ) h16 ] "::" ls32
            / [ *5( h16 ":" ) h16 ] "::" h16 / [ *6( h16 ":" ) h16 ] "::"
ls32        = ( h16 ":" h16 ) / ipv4-number  ; les 32 bits de moindre pois d'adresse IPv6
h16         = 1*4HEXDIG
port        = 1*DIGIT
iscsi-name  = iscsi-char                    ; nom de cible iSCSI
identity    = iscsi-char                    ; chaîne d'identité facultative
iscsi-char  = ALPHA / DIGIT / escaped / ":" / "-" / "."    ; destiné à permettre les chaîne codées en UTF-8.
escaped     = 1*("\" HEXDIG HEXDIG)
```

; La partie iscsi-name de l'URL est exigée et doit être le nom iSCSI de la cible enregistrée. Un appareil qui représente plusieurs cibles doit enregistrer individuellement chaque combinaison cible/adresse auprès de SLP. La partie identité de l'URL est facultative, et est utilisée pour indiquer une identité qui est autorisée à accéder à cette cible. ;
; Exemple : service:iscsi:cible://192.0.2.3:3260/iqn.2001-04.com.exemple:sn.45678
; Les adresses IPv6 sont aussi prises en charge ; elles utilisent la notation spécifiée ci-dessus et au paragraphe 2.2 de la [RFC3513] ;

iscsi-name = string # Le nom iSCSI de cette cible. Cela doit correspondre au iscsi-name dans le url-path.

portal-group = entier
# Étiquette de groupe portail iSCSI pour cette adresse. Les adresses qui partagent le même iscsi-name et étiquette portal-group peuvent être utilisées dans la même session iSCSI. Les groupes Portal sont décrits dans la [RFC3720].

transports = chaîne M L
tcp
# C'est une liste de protocoles de transport que l'entité enregistrée prend en charge. iSCSI est actuellement pris en charge sur TCP, mais il est prévu qu'il pourrait être pris en charge sur d'autres transports, comme SCTP, à l'avenir.
tcp

mgmt-entity = chaîne O
# Nom de domaine pleinement qualifié, ou adresse IP, en notation décimale séparée par des points, de l'interface de gestion de l'entité qui contient cette cible. #

alias = chaîne O # La chaîne alias contient un nom descriptif de la cible.

auth-name = chaîne M X
# Liste de noms d'initiateur iSCSI qui peuvent accéder à cette cible. Les noms iSCSI normaux seront de 80 caractères ou moins ; la longueur maximale est 255. Normalement, seules une ou quelques valeurs seront dans la liste. Utiliser la recherche équivalente sur cela va s'évaluer à "vrai" si un des éléments de cette liste correspond à l'interrogation. Si cette liste contient le nom par défaut "any", tout initiateur à la permission d'accès à cette cible, pourvu qu'elle corresponde aux autres attributs auth-xxx. Cet attribut contient les informations de politique de sécurité. Si cet attribut est distribué via un message Réponse d'attribut, IPsec DOIT être mis en œuvre.

auth-addr = chaîne M X
# Liste d'adresses IP d'initiateurs (ou noms d'hôtes) à qui il sera permis d'accéder à cette cible. Si cette liste contient le nom par défaut de "any", toute adresse IP a la permission d'accéder à cette cible, pourvu qu'elle corresponde aux autres attributs auth-xxx. Cet attribut contient les informations de politique de sécurité. Si cet attribut est distribué via un message Réponse d'attribut, IPsec DOIT être mis en œuvre.

auth-cred = chaîne M X
# liste d'accréditifs qui auront la permission d'accès à la cible (pourvu qu'ils puissent fournir le mot de passe correct ou un autre authentificateur). Les entrées dans cette liste sont de la forme "méthode/identifiant", où les méthodes actuellement définies sont "chap" et "srp", qui prennent tous deux des noms d'utilisateur comme identifiants. Cet attribut contient les informations de politique de sécurité. Si cet attribut est distribué via un message Réponse d'attribut, IPsec DOIT être mis en œuvre.

boot-list = chaîne M O
# Liste de noms d'intiateurs iSCSI qui peuvent s'amorcer à partir de cette cible. Cette liste fonctionne précisément comme l'attribut auth-name. Un nom qui apparaît dans cette liste doit soit apparaître dans la liste d'accès, soit la liste d'accès doit contenir le nom d'initiateur "iscsi". Autrement, un initiateur sera incapable de trouver sa cible de connexion. Si boot-list contient le nom "iscsi", tout hôte peut se connecter à partir d'elle, mais il n'est pas sûr que ceci soit d'une quelconque utilité. Si cet attribut n'est pas enregistré, cette cible n'est pas "amorçable". Noter que le numéro d'unité logique (LUN, *Logical Unit Number*) d'où l'hôte s'amorce n'est pas spécifié ici ; un hôte va généralement tenter de s'amorcer à partir de LUN 0. Il est possible qu'il soit nécessaire de définir aussi d'autres attributs pour l'amorçage. Cet attribut contient les informations de politique de sécurité. Si cet attribut est distribué via un message Réponse d'attribut, IPsec DOIT être mis en œuvre.

----------le gabarit se termine ici----------

### 5.3 Gabarit de service de gestion de mémorisation iSCSI

Ce gabarit définit le service "service:iscsi:sms". Une entité qui prend en charge un ou plusieurs protocoles de services iSCSI de gestion peut s'enregistrer auprès de SLP comme ce type de service. Les clients et serveurs iSCSI qui souhaitent découvrit les services de gestion de mémorisation en utilisant SLP vont généralement les chercher avec les protocoles qu'ils prennent en charge :
Service : service:iscsi:sms
Portée : initiator-scope-list
Interrogation : (protocols=isns)

Nom du soumettant : Mark Bakke
Langage du gabarit de service : en
Considérations de sécurité : voir la Section 6.

Texte du gabarit :
----------le gabarit commence ici----------
template-type=iscsi:sms
template-version=1.0

template-description=
C'est un type de service concret. Le type de service iscsi:sms donne aux entités qui prennent en charge iSCSI la capacité de découvrir les services de gestion appropriés.

template-url-syntax=
url-path = ; URL du service de gestion [RFC2608].
protocols = chaîne M
# Liste des protocoles acceptés par ce service de noms. Cette liste peut être étendue à l'avenir. Il n'y a pas de valeur par défaut. #
# "isns" - Ce service de gestion accepte l'utilisation du protocole iSNS pour la gestion d'accès, la surveillance de la santé, et la découverte des services de gestion. Ce protocole est défini dans la [RFC4171].
isns

transports = chaîne M L
tcp
# C'est une liste de protocoles de transport que l'entité enregistrée prend en charge.
tcp, udp

server-priority = entier
# Priorité qu'un client devrait accorder à ce serveur, lors d'un choix entre plusieurs serveurs avec le même type de protocole. Lorsque plusieurs serveurs sont découverts pour un certain type de protocole, ce paramètre indique leurs préséances relatives. La préséance de serveur est spécifique du protocole ; pour certains protocoles, le serveur principal peut avoir la plus haute valeur de priorité de serveur, tandis que pour d'autres il peut avoir la plus faible. Par exemple, avec iSNS, le serveur principal a la plus faible valeur (valeur 0).

----------le gabarit se termine ici----------

## 6. Considérations sur la sécurité

Le modèle de sécurité SLPv2 tel que spécifié dans la [RFC2608] n'assure pas la confidentialité mais fournit un mécanisme d'authentification pour les UA pour s'assurer que les annonces de service ne viennent que de SA de confiance, sauf qu'il ne fournit pas de mécanisme pour authentifier les "réponses de résultat zéro". Voir dans la [RFC3723] une discussion du modèle de sécurité de SLPv2 [RFC2608].

Une fois qu'une cible ou un serveur de gestion est découvert, l'authentification et l'autorisation sont traitées par le protocole iSCSI, ou par le protocole du serveur de gestion. Il est de la responsabilité des fournisseurs de ces services de s'assurer qu'un service annoncé ou découvert de façon inappropriée ne compromet par leur sécurité.

Lorsque aucune sécurité n'est utilisée pour SLPv2, il y a un risque de distribution de fausses informations de découverte. La principale contre mesure pour ce risque est l'authentification. Si ce risque pose un problème significatif, on DEVRAIT utiliser les associations de sécurité IPsec et l'authentification iSCSI dans la bande pour le trafic iSCSI soumis à ce risque pour s'assurer que le trafic iSCSI ne s'écoule qu'entre des points d'extrémité qui ont participé à l'authentification IKE et à

l'authentification iSCSI dans la bande. Par exemple, si un attaquant distribue de fausses informations de découverte prétendant qu'il est une cible iSCSI, il lui manquera les informations secrètes nécessaires pour effectuer avec succès l'authentification IKE ou l'authentification iSCSI dans la bande et sera donc empêché d'envoyer ou recevoir du trafic iSCSI.

Il reste un risque d'attaque de déni de service sur la base de l'utilisation répétée de fausses informations de découverte qui vont causer l'initiation d'une négociation IKE. Les contre mesures sont la configuration administrative de chaque cible iSCSI à limiter les homologues avec lesquels elle accepte de communiquer (c'est-à-dire, par gamme d'adresses IP et/ou domaines DNS) et la tenue d'une antémémoire d'authentification négative pour éviter de contacter de façon répétitive une cible iSCSI qui échoue à s'authentifier. Ces trois mesures (c'est-à-dire, limite de gamme d'adresses IP, limites de domaines DNS, antémémoire d'authentification négative) DOIVENT être mises en œuvre.

Les attributs auth-name, auth-addr, auth-cred, et boot-list comportent des informations de politique de sécurité. Lorsque ces attributs sont distribués, IPsec DOIT être mis en œuvre.

### 6.1 Mise en œuvre de la sécurité

La sécurité pour SLPv2 dans un environnement de mémorisation IP est spécifiée dans la [RFC3723]. IPsec est de mise en œuvre obligatoire pour les clients et serveurs IPS. Donc, tous les clients de mémorisation IP, incluant ceux qui invoquent SLP, peuvent être supposés prendre en charge IPsec. Cependant les serveurs SLP ne peuvent pas être supposés mettre en œuvre IPsec, car il n'y a pas cette exigence dans le SLP standard. En particulier, les agents de répertoire (DA, *Directory Agent*) SLP peuvent fonctionner sur des machines autres que celles qui font fonctionner les protocoles IPS.

IPsec DEVRAIT être mis en œuvre pour SLPv2 comme spécifié dans la [RFC3723] ; ceci inclut ESP avec une transformation non nulle pour fournir à la fois l'authentification et la confidentialité.

Lorsque SLPv2 peut être utilisé pour distribuer les informations de auth-name, auth-addr, auth-cred, et boot-list (voir le paragraphe 5.2) IPsec DOIT être mis en œuvre, car ces éléments sont considérés comme des informations de politique de sécurité sensibles. Si IPsec n'est pas mis en œuvre, les informations de auth-name, auth-addr, auth-cred, et boot-list NE DOIVENT PAS être distribuées via SLPv2 et NE DOIVENT PAS être utilisées si elles sont découvertes via SLPv2.

Parce que les services de mémorisation IP ont leurs propres capacités d'authentification lorsque ils sont localisés, l'authentification SLPv2 est de mise en œuvre et d'utilisation FACULTATIVES (comme discuté plus en détails dans la [RFC3723]).

## 7. Considérations relatives à l'IANA

Le présent document décrit trois gabarits SLP. Ils ont été revus et approuvés par l'IESG et enregistrés dans le registre "SVRLOC Templates" de l'IANA. Ce processus est décrit dans la section "Considérations relatives à l'IANA de la [RFC2609].

## 8. Résumé

Le présent document décrit comment SLP peut être utilisé par les initiateurs iSCSI pour trouver des cibles iSCSI et des serveurs de gestion de mémorisation. Il présente les gabarits de type de service pour les cibles iSCSI et pour les serveurs de gestion de mémorisation.

## 9. Références normatives

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

[RFC2608] E. Guttman et autres, "Protocole de localisation de service, version 2", juin 1999. (*MàJ par* RFC3224) *(P.S.)*

[RFC2609] E. Guttman, C. Perkins, J. Kempf, "Schémas service: et gabarits de service", juin 1999. *(P.S.)*

[RFC3491] P. Hoffman et M. Blanchet, "Nameprep : Profil Stringprep pour les noms de domaine internationalisés (IDN)", mars 2003. (*Remplacée par la* RFC5891, *P.S.*)

[RFC3513] R. Hinden et S. Deering, "Architecture d'adressage du protocole Internet version 6 (IPv6)", avril 2003. (*Obs. voir* RFC4291)

[RFC3720] J. Satran et autres, "Interface Internet des systèmes de petits ordinateurs (iSCSI)", avril 2004. *(Remplacée par* RFC7143)

[RFC3722] M. Bakke, "Profil de chaîne pour les noms d'interface Internet de systèmes de petits ordinateurs (iSCSI)", avril 2004. *(P.S.)*

[RFC3723] B. Aboba et autres, "Protocoles de sécurisation de mémorisation de blocs sur IP", avril 2004. *(P.S.)*

## 10. Références pour information

[RFC2614] J. Kempf, E. Guttman, "API pour la localisation de service", juin 1999. *(Information)*

[RFC3105] J. Kempf et G. Montenegro, "Trouver un serveur RSIP avec SLP", octobre 2001.

[RFC3721] M. Bakke et autres, "Interface Internet des systèmes de petits ordinateurs (iSCSI) : dénomination et découverte", avril 2004. *(Information) (MàJ par* RFC7143)

[RFC4171] J. Tseng et autres, "Service de noms de mémorisation sur Internet (iSNS)", septembre 2005. *(P.S.)*

[RFC4173] P. Sarkar et autres, "Clients d'amorçage qui utilisent le protocole d'interface de système de petit ordinateur sur Internet (iSCSI)", septembre 2005. *(P.S.)*

[SAM2] ANSI T10. "SCSI Architectural Model 2", mars 2000.

## 11. Remerciements

Le présent document a été produit par l'équipe Désignation et découverte iSCSI composée de Joe Czap, Jim Hafner, John Hufferd, et Kaladhar Voruganti (IBM), Howard Hall (Pirus), Jack Harwood (EMC), Yaron Klein (Sanrad), Marjorie Krueger (HP), Lawrence Lamers (San Valley), Todd Sperry (Adaptec), et de Joshua Tseng (Nishan). Merci aussi à Julian Satran (IBM) qui a suggéré l'utilisation de SLP pour la découverte iSCSI, et à Matt Peterson (Caldera) et James Kempf (Sun) pour leur relecture du document du point de vue de SLP.

## Adresse des auteurs

Mark Bakke
Cisco Systems, Inc.
7900 International Drive, Suite 400
Bloomington, MN
USA 55425
mél : mbakke@cisco.com

Kaladhar Voruganti
IBM Almaden Research Center
650 Harry Road
San Jose, CA 95120
mél : kaladhar@us.ibm.com

John L. Hufferd
IBM Storage Systems Group
5600 Cottle Road
San Jose, CA 95193
téléphone : +1 408 997-6136
mél : jlhufferd@comcast.net

Marjorie Krueger
Hewlett-Packard Corporation
8000 Foothills Blvd
Roseville, CA 95747-5668, USA
téléphone : +1 916 785-2656
mél : marjorie_krueger@hp.com

Todd Sperry
Adaptec, Inc.
691 South Milpitas Boulevard
Milpitas, Ca. 95035
téléphone : +1 408 957-4980
mél : todd_sperry@adaptec.com

## Déclaration complète de droits de reproduction

pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations qui y sont contenues sont fournis 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 l'Internet Society.