Internet Engineering Task Force
INTERNET DRAFT
July 6, 2000
Expires in six months

Erik Guttman
James Kempf
Sun Microsystems

Proposed Modifications to the Service Location Protocol, Version 2

<draft-guttman-svrloc-slpv2bis-01.txt>

Status of this Memo

Abstract

SLPv2 [1] has been widely implemented but not all features of the protocol are in common use. If these features were deprecated from the specification the protocol would be simpler, yet still perform its core function. The changes proposed in this document could be the basis for a revision of SLPv2 as it is considered for advancement to Draft Standard.

This draft incorporates changes and suggestions from the SVRLOC WG mailing list.

1. Introduction

SLPv2 has been widely implemented but not all features of the protocol are in common use. If these features were deprecated from

the specification the protocol would be simpler, yet still perform it core features. The changes proposed in this document could be the basis for a revision of SLPv2 as it is considered for advancement to Draft Standard.

This document begins with the motivation for revision. Specific revisions are proposed. Finally, minimal requirements for SLPv2bis compliant hosts are summarized.

Changes proposed in this document will not modify any of the SLPv2 on-the-wire protocol. Features will be dropped and in a couple cases slightly new interpretations of rules are given.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [2].

1.1 Summary of SVRLOC WG mailing list discussion on SLPv2bis

The following is section 1.1 from the document, which enumerates the changes from 1.0 with commentary drawn from the mailing list.

. PR Lists - deprecate them?

  No. PR Lists are effective and important in practice.
  ---Kevin Arnold: http://www.srvloc.org/hypermail/0605.html

  We *could* use Exclusion Lists - but they require security.
  Maybe if they were defined only for a single source addr/port/xid
  we could use them without security. Exclusion lists scale *far
  better* but require state to be kept on SAs and DAs.
  ---Michael Day: http://www.srvloc.org/hypermail/0584.html

. Search filter issue #1: Limit requests to either one term or a list of conjoined terms. Disallow '!' and '|' operations.

  The '!' filter is really complex to implement.
  ---James Kempf: http://www.srvloc.org/hypermail/0596.html

  Maintaining compatibility with LDAP filters is critical (so
  that LDAP servers can back-end DAs and SAs and LDAP search
  filter code can be used verbatim.)
  ---Terry Lambert: http://www.srvloc.org/hypermail/0575.html

. Search filter issue #2: Limit requests to '=' comparisons, (not '<=', '>=', '=*', '~=').

  No. Search filters reduce traffic on the net.

---Evan Hughes: http://www.srvloc.org/hypermail/0568.html

No. It scales poorly to have UAs gather attributes to do local compares.
---Evan Hughes: http://www.srvloc.org/hypermail/0576.html
---Terry Lambert: http://www.srvloc.org/hypermail/0575.html

No. Load balancing is a critical application which requires <= and >=
---Terry Lambert: http://www.srvloc.org/hypermail/0575.html

. Search filter issue #3: Disallow wildcards in search filters like (x=some words follow*)

No. There are applications which require them.
---Mikael Pahmp: http://www.srvloc.org/hypermail/0609.html

There was no disagreement, so I will keep the following changes:

. Recommend mesh enhanced support to DAs.

This will require that mSLP be advanced as a proposed standard.
---Erik Guttman: http://www.srvloc.org/hypermail/0616.html

. Deprecate attribute tag list wildcards

. Deprecate service deregistration tag list wildcards

. Deprecate attribute requests by type.

. Deprecate RFC 2610 MANDATORY scope flags

. Use MADCAP nested scope option

. Change the scope configuration rules

. Use literal string matching (not requiring elision of spaces)

2.0 Motivation

There are four features which made SLPv2 complicated to implement.

- SAs and DAs MUST implement full LDAPv3 search filters [3] for matching service requests. This required complex parsing and indexing. See Section 3.1.

- Attribute Requests by service type was difficult to collate. See Section 3.2.

- SAs MUST keep track of all DAs it discovers and forward SrvReg and SrvDereg messages to each of them. This requires the SA to

passively discover DAs and to maintain and act on non-trivial

state information. See Section 3.3.

- Previous Responder Lists made message headers variable length for each retransmission. See Section 3.4.

Some of these features have proven to be unnecessary. In fact many implementations have foregone them.

There are other features which were viewed as useful during the design phase of SLPv1 which have not proven their worth in deployment and have burdened the protocol unnecessarily.

3.0 Recommended Modifications of SLPv2

The following section details all suggested changes to the protocol.

3.1 Service Request

3.1.1. Limit requests to at most 1 '&' logical operator. Thus, only requests of type (x=4) or (&(x=4)(y=3)) are allowed.

The result of these rules will be that SLPv2 search filters will be compatible with LDAPv3 search filter, but not visa versa. A compliant LDAPv3 search filter implementation will be able to process LDAPv3-subset search filters, but a SLPv2 compliant implementation will not be able to process an arbitrary LDAPv3 search filter.

Complicated logical queries for services have not proven useful. Allowing conjunctions of required attributes has proven very useful and is easy to implement.

3.2 Attribute Request

3.2.1. Eliminate attribute requests by type. Attribute requests will be by service URL only.

3.2.2. Eliminate wild cards in attribute request search filters.

Attribute requests for service by type have proven difficult to implement and interpret. This feature should be deprecated.

3.3 DA Discovery

3.3.1. Recommend that DAs do mesh enhancement [7].

Mesh enhanced DAs add very little complexity to DAs. If even one

is present in a given scope, a SA does not need to keep track of other DAs in that scope. Forwarding to the mesh enhanced DA will

effectively cause a registration to be forwarded to all DAs in that scope.

3.4 Transport

3.4.1. Propose a new Exclusion List Extension. This could be used instead of PR Lists.

An Exclusion List tells a SA or a DA not to respond to the requester (identified by their address, source port number and XID of the request) for a some period of time. This scales to far more hosts than a PR list, since successive requests can be issued.

One problem is that some authentication is required in order to prevent a trivial denial of service attack.

Another problem is that not all SAs and DAs will support this option unless it is required. In that case, PR lists would still be needed.

3.5 Scope Configuration

3.5.1. Deprecate MANDATORY flags in RFC 2610.

3.5.2. Use nested scopes in MADCAP [5] for scope config. SAs and DAs join all groups at the top of each nested scope (address range). They advertise all scopes by the name received in the MADCAP Nested Scope Option [6].

3.5.3. The simplified scope configuration list would be in decreasing order of preference

Pref	Feature	Requirement 'mode'
1)	static configuration of scope list	MUST
2)	static configuration of DAs*	MUST
3)	dhcp configuration	SHOULD
4)	dhcp configuration of DAs*	SHOULD
5)	MADCAP / scope configuration	SHOULD
6)	dynamic discovery (DAAdverts)**	MAY
7)	dynamic discovery (SAAdverts)**	MAY
8)	Use of the scope "default"	MUST

The higher item on the list always takes precedence over the lower items. If no other configuration is supplied, a SLP Agent is configured with the scope list "default".

* If a scope list is not configured (by through static configuration

or DHCP) but a list of DAs is, the SLP Agent MUST unicast a SrvRqst for "service:directory-agent" to each of the DAs on the

list. The SLP Agent is configured with the scope list which is the union of all scopes supported by the DAs which respond with a DAAdvert. If a DA on the configuration list does not respond, the SLP Agent SHOULD try to send it a SrvRqst again periodically (like every 30 minutes). Once a DAAdvert is received, the scope list MAY be expanded and the # of DAs known of by the SLP Agent increases.

**Dynamic discovery of scopes MAY be used by User Agents and MUST NOT be used to configure Service Agent or Directory Agent scope lists.

The problem with the current scope rules is that they are overly complicated. This is largely due to the 'MANDATORY' bit in the SLPv2 DHCP Option [9]. A clarification of how to do scope rules using the current specifications shows just how hard it is [10].

Further, when SLPv2 was published, the Administrative Scoping BCP [4] was available, but further specifications were not. Now, with MADCAP and the MADCAP Nested Scope Option it is possible to define specific automatic scope configuration behavior.

3.6 Service Deregistration

3.6.1. Eliminate wild cards in the tag list for selective attribute deregistration.

3.7 String Matching

3.7.1. Eliminate the requirement to elide white space in requests. If white space is included unintentionally on registration or requests - that is an error. Use the templates literally (just don't add unwanted space). This effects every message - scope lists, tag lists, attribute lists, queries, and so on.

Eliding white space allowed requests to be 'sloppy' and still match strings in registered by other servers. In practice this does not seem to be a problem since strings can be trimmed before being registered or before requests are sent. Many strings are will have extra white space due to manual entry anyway.

4.0 Minimal Features

The following minimal features will result from this trimming of SLPv2.

4.1 Directory Agent

- Send DAAdverts periodically
- Respond to service requests for DA with DAAdvert, but only if the DA is not on the service request previous responder list.
- Respond to SrvRqst, AttrRqst and SrvTypeRqst with SrvRply, AttrRply and SrvTypeRqst
- Accept SrvReg and SrvDereg messages
- Age services out of the cache when their lifetimes expire

The following mandatory features for DAs would be dropped due to the proposed revision.

- Handling Attribute Requests by service type.
- Handling wild cards in Service Deregistration tag lists.

For backward compatibility with existing SLPv2 UAs and SAs other features could not be dropped. However, very few SLPv2 DAs have been deployed. It is conceivable that further features (described in section 3) could be made optional for DAs.

4.2 Service Agent

- Active DA discovery (1)
- Passive DA discovery (1)
- Discard requests if the SA's address is on the Previous Responders list
- Respond to service request for SA with SAAdvert
- Respond to service requests for services with SrvRply (2)
- De/Register with discovered DAs (1)

(1) If mesh enhanced DAs have been discovered, only one DA need be registered with. Further passive DA discovery would not be needed once such a DA has been discovered, too.

(2) SAs return a 'not implemented error' if they cannot parse a LDAPv3 search filter. Clients can then infer that the SA can only handle the restricted subset. (Since SLPv2 SAs MUST support SrvRqst - the not implemented refers to the search filter not to the function).

The following mandatory features for SAs would be dropped due to the proposed revision.

- Eliding White Space in requests
- Handling LDAPv3 search filter features ('|' and '!')

4.3 User Agent

- Active DA discovery (1)
- Multicast SrvRqst if no discovered DAs
- Unicast SrvRqst if discovered DAs

(1) Active DA discovery should be done periodically if no DAs discovered initially.

5.0 Backward Compatibility

SLPv2 may be modified to drop features and remain backwardly compatible with the current specification. Only two things need to occur to guarantee this. First, SLPv2 DAs SHOULD remain backwards compatible with RFC 2608 features. Second, SLPv2 UAs and SAs MUST be prepared to accept NOT IMPLEMENTED errors for the features which are being dropped.

The risk of backward compatibility problems is limited because client and server systems (UA and SA pairs) tend to be deployed together to form end-to-end systems. As new UAs and SAs are deployed, they will not attempt to use the deprecated features.

6.0 Security Considerations

The modifications described in this memo would not modify the security considerations for SLPv2 [1] except in so far as they suggest the use of mesh-enhanced registration. Those security considerations are discussed elsewhere [7].

7.0 Acknowledgments

Mikael Pahmp (Axis Communications) contributed very helpful comments which started the process of thinking about how to trim down SLPv2. Thanks to contributors to the SVRLOC WG mailing list discussion (in aphabetical order):

Kevin Arnold, Michael Day, Evan Hughes, Terry Lambert, Ira McDonald, Mikael Pahmp, James Woodyatt

8.0 References

[1] Guttman, E., Perkins, C., Veizades, J., Day, M., "Service Location Protocol, Version 2", RFC 2608, July 1999.

[2] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] Howes, T., "The String Representation of LDAP Search Filters", RFC 2254, December 1997.

[4] Meyer, D., "Administratively Scoped IP Multicast", RFC 2365, July 1998.

[5] Hanna, S., Patel, B., Shah, M., "Multicast Address Dynamic Client Allocation Protocol (MADCAP)", RFC 2730, December 1999.

[6] Kermode, R., "MADCAP Multicast Scope Nesting State Option", <draft-ietf-malloc-madcap-nest-opt-04.txt>, April 2000, A work in progress.

[7] Zhao, W., Schulzrinne, H., "Interaction of SLP Directory Agents for Reliability and Scalability", <draft-zhao-slp-da-interaction-03.txt>, May 2000, A work in progress.

[8] Guttman, E., "Attribute List Extension for the Service Location Protocol", draft-guttman-svrloc-attrlist-ext-02.txt, March 1999, A work in progress.

[9] Perkins, C., Guttman, E., "DHCP Options for Service Location Protocol", RFC 2610 June 1999.

[10] Kempf, J., Pahmp, M., Holm, R., "SLP Scope and DA Configuration", <draft-kempf-scope-rules-03.txt>, December 1999, A work in progress.

9.0 Authors' Contact Information

Erik Guttman
Network and Security Research Center, Sun Laboratories
Sun Microsystems, Inc.
Eichhoelzelstr. 7
74915 Waibstadt
Germany

Phone: +49 172 865 5497
Fax: +49 7263 911 701
Email: Erik.Guttman@Sun.Com

James Kempf
Network and Security Research Center, Sun Laboratories
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, CA 94025
USA

Phone: +1 650 786 5890

Fax: +1 650 786 6445
Email: James.Kempf@Sun.Com

10. Full Copyright Statement