Network Working Group
Request for Comments: 3105
Category: Experimental

J. Kempf
NTT DoCoMo USA Labs
G. Montenegro
Sun Microsystems
October 2001

Finding an RSIP Server with SLP

Status of this Memo

Copyright Notice

IESG Note

The IESG notes that the set of documents describing the RSIP technology imply significant host and gateway changes for a complete implementation. In addition, the floating of port numbers can cause problems for some applications, preventing an RSIP-enabled host from interoperating transparently with existing applications in some cases (e.g., IPsec). Finally, there may be significant operational complexities associated with using RSIP. Some of these and other complications are outlined in section 6 of the RFC 3102, as well as in the Appendices of RFC 3104. Accordingly, the costs and benefits of using RSIP should be carefully weighed against other means of relieving address shortage.

Abstract

This document contains an SLP service type template that describes the advertisements made by RSIP servers for their services. Service Location Protocol (SLP) is an IETF standards track protocol specifically designed to allow clients to find servers offering particular services. Since RSIP (Realm Specific IP) clients require a mechanism to discover RSIP servers, SLP is a natural match for a solution. The service type template is the basis for an Internet Assigned Numbers Authority (IANA) standard definition of the advertisements offered by RSIP servers, an important step toward interoperability.

Table of Contents

1. Introduction

Realm Specific IP (RSIP) [7] enables an RSIP client in one realm to borrow addresses and other resources from another realm. It does so by engaging in an RSIP protocol [1] exchange with an RSIP server. The RSIP protocol requires the RSIP server to have a permanent presence on both realms.

There are a variety of traditional ways an RSIP client could go about locating the appropriate RSIP server. However, Service Location Protocol (SLP) [2][11] is an IETF standards track protocol specifically designed to facilitate location of services and their servers by clients. SLP provides a number of features that simplify locating RSIP servers. In this document, we describe how RSIP clients can use SLP to discover RSIP servers.

2. Notation Conventions

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 [4].

3. Terminology

We reproduce here some SLP terminology from [2] for readers unfamiliar with SLP.

User Agent (UA)

A process working on the user’s behalf to establish contact with some service. The UA retrieves service information from the Service Agents or Directory Agents.

Service Agent (SA)

A process working on behalf of one or more services to advertise the services and their capabilities.

Directory Agent (DA)

A process which collects service advertisements. There can only be one DA present per given host.

Scope

A set of services, typically making up a logical administrative group.

Service Advertisement

A URL, attributes, and a lifetime (indicating how long the advertisement is valid), providing service access information and capabilities description for a particular service.

4. Using SLP for RSIP Service Discovery

SLP provides the framework in which RSIP clients and servers make contact. Here is a description of how an RSIP server and client find each other using SLP:

1. The RSIP server implements a SLP SA while the RSIP client implements an SLP UA.

2. The RSIP SA constructs a service advertisement consisting of a service URL, attributes and a lifetime. The URL has service type "service:rsip", and attributes defined according to the template in Section 7.

3. If an SLP DA is found, the SA contacts the DA and registers the advertisement. If no DA is found, the SA maintains the advertisement itself, answering multicast UA queries directly.

4. When the RSIP client requires contact information for an RSIP server, the UA either contacts the DA using unicast or the SA using multicast. The UA includes a query based on the attributes to indicate the characteristics of the server it requires.

5. Once the UA has the host name or address of the RSIP server as well as the port number, it can begin negotiation using the RSIP protocol.

This procedure is exactly the same for any client/server pair implementing SLP and is not specific to RSIP.

Many protocols use a variety of traditional methods for service discovery. These methods include static configuration, purpose-build protocols for discovery, special features in the protocol itself, DNS SRV RRs [5], or DHCP [6]. SLP provides a number of advantages over these traditional methods:

1. Discovery of services using SLP is dynamic, whereas many of the traditional methods only allow static or weakly dynamic (i.e., difficult to update) discovery. Clients only discover services that are actually active with SLP. Furthermore, if subsequent to initial discovery a server goes down, the client can reissue an SLP query and obtain a new server. On the server side, no databases must be updated to provide dynamic discovery, the servers advertise themselves.

2. SLP requires no third party configuration. Only the server offering the service and the client seeking it are required to know the details for the particular service type.

3. SLP allows clients to specify the attributes describing the desired server. A client discovers servers that meet a set of specific requirements. This reduces the amount of network traffic involved in selecting a server when many possible choices are available.

4. SLP contains a number of scaling mechanisms (DAs, scopes, multicast convergence algorithm), that facilitate deployment in large enterprise networks as well as in smaller networks.

5. Using Scopes for Server Provisioning

One particular design feature of SLP that is useful for RSIP is scopes. Scopes in SLP are a mechanism for provisioning access to particular service advertisements. An administrator assigns UAs and SAs to particular scopes to assure that UAs only find SAs in those scopes. Scopes are not an access control mechanism for the service itself, however. UAs from outside the scope can still access services in a particular scope (unless the service itself provides for access control), they just won’t be able to find the services using SLP.

Scopes are useful for RSIP service advertisement provisioning because they allow a system administrator to tie particular RSIP clients to specific RSIP servers. For example, consider the network architecture described in Section 4.2.1 of [7]. RSIP clients are recommended to find "the nearest" RSIP server, but exactly how that should be arranged is left unspecified. SLP provides a way for system administrators to precisely specify which realm an RSIP client resides in, by tying the realm to an SLP scope. The diagram from Section 14.1 is reproduced here, with SLP scopes included to illustrate how clients could be directed to the right RSIP servers.

```
                                +-----------+
                                |           |
                                |   RSIP    |
                                |  server   +---- 10.0.0.0/8
                                |     B     |   SLP Scope: B
                                |           |
                                +-----+-----+
                                      |
                                      | 10.0.1.0/24
                       +-----------+  | (149.112.240.0/25)
                       |           |  |
       149.112.240.0/24|    RSIP   +--+
       ----------------+   server  |    SLP Scope: A
                       |      A    +--+
                       |           |  |
                       +-----------+  | 10.0.2.0/24
                                      | (149.112.240.128/25)
                                      |
                                +-----+-----+
                                |           |
                                |   RSIP    |
                                |  server   +---- 10.0.0.0/8
                                |     C     |     SLP Scope: C
                                |           |
                                +-----------+
```

Clients on the upper 10.0.0.0/8 network are configured to use SLP scope B, while clients on the lower 10.0.0.0/8 network are configured to use SLP scope C. RSIP servers B and C (as clients of server A) use SLP to locate RSIP server A, as do other RSIP clients on the 10.0.1.0/24 and 10.0.2.0/24 subnets. Within these two subnets, all clients have their scopes configured to be A.

Note that specifying a particular SLP scope for RSIP clients does not restrict the SLP scope for other services advertised by SLP. SLP UAs can be configured for multiple scopes, so the scope configured for printing may be different from the scope configured for RSIP service.

Since SLP scopes are configured through a DHCP option [8], along with the IP address, system administrators can easily switch a cluster of machines from one realm to another by simply changing the scope and

IP address assignments on the DHCP server. For example, in the above architecture, suppose a system administrator wanted to remove RSIP server B so that clients on the upper 10.0.0.0/8 subnet were directly on subnet 10.0.1.0/24. These clients now communicate with RSIP server A. By simply changing the address assignments and scope configuration of these clients on the DHCP server, the realm can be effectively switched.

6. Load Balancing

While SLP itself contains no specific provision for load balancing, load balancing can easily be implemented using SLP. The only requirement is that the service type template specify an attribute indicating server load. In the case of RSIP, the service type template in Section 7 contains such an attribute. The attribute indicates the number of RSIP client sessions currently being supported by the server.

In order to perform load balancing, the RSIP server must update its service advertisement periodically as new connections are accepted. An RSIP client seeking to find the server having the lightest load performs the following series of SLP operations.

1. As in Section 4, the client issues an SLP service request and collects all the returned service URLs.

2. For each service URL, the client performs an SLP attribute request for the attribute LOAD. The integer load figures are returned.

3. The client sorts through the returned load figures and selects the URL having the least number of connections. The client establishes its RSIP session with that server.

Because of network delays, this procedure does not guarantee that a client will always obtain a connection with the lightest loaded server, but it does provide a high probability that the selected server is more lightly loaded.

A similar procedure is used in [9] to load balance access to TN3270E telnet servers.

7. The RSIP Service Type Template

Name of submitters: James Kempf <james@docomolabs-usa.com>
Gabriel Montenegro <gab@sun.com>

Language of service template: en

Security Considerations:
RSIP clients can use Service Location Protocol to find RSIP servers having particular security characteristics. If secure access to such information is required, SLP security should be used.

Template text:

```
----------------------template begins here ------------------------
template-type = rsip

template-version = 0.0

template-description=
   The service:rsip type provides advertisements for clients seeing
   realm-specific IP (RSIP) servers.  RSIP servers use the Realm
   Specific IP protocol to manage addresses and other resources
   from one realm on behalf of a client in another realm.

template-url-syntax=
   ;No additional URL path information required.  An example service
   ;URL for an RSIP server is: service:rsip://gateway.mydomain:4455

ipsec-support = BOOLEAN O
   #True if the server supports IPSEC as per [10]

ike-support = BOOLEAN O
   #True if the server supports IKE as per [10]

tunnel-type = STRING L M O
IP-IP
   #The tunneling methods supported by the RSIP server.  Clients
   #should include this attribute in a query so that they obtain a
   #server offering a tunneling method for which they have
   #support.  Default is IP-IP.  The values are currently
   #restricted to IP-IP, L2TP, GRE and NONE.  A server can support
   #multiple tunnel types.
IP-IP,L2TP,GRE,NONE

transport = STRING L M O
TCP
   #Transport used by the RSIP protocol itself.
TCP,UDP

load = INTEGER O
   #If the server supports load balancing, this attribute should be
   #set to an integer from 0 to 100.  0 is the lowest indication of
   #load and 100 the highest.  Clients can query for this attribute
   #and obtain load information, from which they can make an
   #intelligent decision about which server to use.
----------------------template ends here --------------------------
```

8. Security Considerations

Service type templates provide information that is used to interpret information obtained by clients through SLP. If the RSIP template is modified or if a false template is distributed, RSIP servers may not correctly register themselves, or RSIP clients may not be able to interpret service information.

SLP provides an authentication mechanism for UAs to assure that service advertisements only come from trusted SAs [2]. If trust is an issue, particularly with respect to the information sought by the client about IPSEC and IKE support, then SLP authentication should be enabled in the network.

9. Summary

This document describes how SLP can be used by RSIP clients to find RSIP servers. A service type template for an RSIP SLP service type is presented. In addition, a few techniques for provisioning access to service advertisements for particular gateway servers, and for load balancing using SLP were provided. The result should allow RSIP service provisioning that is considerably more dynamic and robust than when traditional service discovery mechanisms are used.

References

[1] Borella, M., Grabelsky, D., Lo, J. and K. Taniguchi, "Realm Specific IP: Protocol Specification", RFC 3103, April 2001.

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

[3] Guttman, E, Perkins, C. and J. Kempf, "Service Templates and service: Schemes", RFC 2609, July 1999.

[4] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] Gulbrandsen, A. and P. Vixie, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2052, October 1996.

[6] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[7] Borella, M., Lo, J., Grabelsky, D. and G. Montenegro, "Realm Specific IP: Framework", RFC 3102, October 2001.

[8] Perkins, C. and E. Guttman, "DHCP Options for Service Location Protocol", RFC 2610, July 1999.

[9] Naugle, J., Kasthurirangan, K. and G. Ledford, "TN3270E Service Location and Session Balancing", RFC 3049, January 2001.

[10] Montenegro, G. and M. Borella, "RSIP Support for End-to-end IPSEC", RFC 3104, October 2001.

[11] E. Guttman, "Service Location Protocol: Automatic Discovery of IP Network Services," IEEE Internet Computing, July/August 1999. Available at: http://computer.org/internet/ic1999/w4toc.htm

Authors’ Addresses

Questions about this document may be directed to:

James Kempf
NTT DoCoMo USA Labs
181 Metro Drive, Suite 300
San Jose, CA
95110

Phone: 408-451-4711
Email: james@docomolabs-usa.com

Gabriel E. Montenegro
Sun Microsystems
Laboratories, Europe
29, chemin du Vieux Chene
38240 Meylan
FRANCE

Phone: +33 476 18 80 45
EMail: gab@sun.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.