Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 4, 2013

Z. Chen
China Telecom
C. Zhou
Huawei Technologies
T. Tsou
Huawei Technologies (USA)

July 3, 2012

The Syslog Requirements to Support NAT Log in Traceback Solutions
draft-zhou-behave-syslog-nat-logging-00

Abstract

This document describes the syslog information that are required for NAT logging. The document will define the NAT logging server which supports traceback and explain the procedure of network location and service support for traceback. The requirements of syslog interface and Radius interface to support NAT log are introduced.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 4, 2013.

Table of Contents

1. Introduction 3
1.1. Traceback Solutions 3
1.2. The Log Server Function 3
2. Terminology 4
3. The Requirements of Log Server Function 4
4. The Log Server Interface Requirements 5
4.1. Syslog Interface 5
4.1.1. Definition of HEADER Part 5
4.1.1.1. PRI 5
4.1.1.2. VERSION 7
4.1.1.3. TIMESTAMP 7
4.1.1.4. HOSTNAME 7
4.1.1.5. APP-NAME 7
4.1.1.6. PROCID 7
4.1.1.7. MSGID 7
4.1.2. Definition of MSG Part 8
4.1.3. Examples 8
4.2. The Radius Interface Requirements 9
5. The Performance Requirements of The Log Server 10
6. The Reliability Requirements of The Log Server 10
7. IANA Considerations 11
8. Security Considerations 11
9. Normative References 11
Authors' Addresses 11

1. Introduction

1.1. Traceback Solutions

In the existing IPv6 transition technology, there are two ways of address and port mapping:static mapping and dynamic mapping. Based on this, we summarize four traceback solutions:

1. After the address and port mapping information is created, NAT device (e.g.,Carrier Grade NAT) sends the syslog mapping information to the log server. AAA system acquires the dynamic address mapping information from the syslog server when receiving traceback request.

2. NAT device reports the dynamic mapping information to AAA system via radius protocol. AAA system will record the subscriber online information and source session list. After traceback request is received, AAA system will return the trackback result with the subscriber online information and source session list information.

3. NAT device reports the dynamic mapping information to the log server through radius protocol. AAA system acquires the mapping information from syslog server when receiving the traceback request.

4. AAA system and NAT device send the parameters through network configuration system and perform the same mapping algorithm to generate address and port. In the traceback procedure, there is no need for AAA system and NAT device to transmit the mapping information.

In solution 1 and 3, the traceback log server will be a newly created device.

1.2. The Log Server Function

The traceback log server receives, analyzes and stores the address/ port address mapping information sent by NAT devices. The logic illustration of the log server is shown in Figure 1.

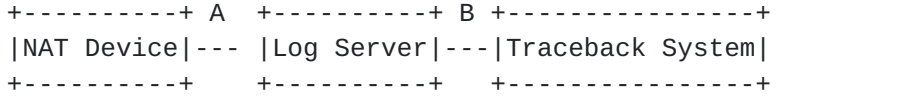

Figure 1: Location Of Log Server In The Network

The log server acquires dynamic address/port mapping information from

the NAT device via interface A, and provides the mapping information to the traceback system (or AAA) via interface B.

2. Terminology

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 "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119].

:Logging information: In this document, this specifically means dynamic address/port mapping logging information.

3. The Requirements of Log Server Function

This section defines the basic requirements for the log server.

- It MUST support The Syslog Protocol [RFC5424].
- It MUST support Transport Layer Security (TLS) Transport Mapping forSyslog [RFC5425].
- It MUST support Transmission of Syslog Messages over UDP [RFC5426]. The log server must support sending the syslog log using standard UDP port 514, and support sending syslog log using any one self-configured port of the user.
- It is suggested to support Reliable Delivery for Syslog [RFC3195].
- It MUST support the Radius message format defined in [RFC2865] or [RFC2866].
- It MUST support acquiring user's dynamic address/port mapping information from NAT device.
- It MUST support the functions of log query, storage, filter, duplication removal, collection and statistic analysis.
- The storage information of the log server MUST include the following information, but not limited to:
  - Application name
  - Hostname

* Start time
* Original source IP
* Translated source IP
* Translated source start port
* Translated source stop port

4. The Log Server Interface Requirements

The log server MUST select one interface between syslog and radius to communicate with NAT device. It MUST provide the query interface to the traceback system.

4.1. Syslog Interface

The syslog message includes two parts: the HEADER and the MSG. The packet records the device operation using ASCII text, and the length of the packet should not exceed 1024 bytes. The minimum length of the syslog message is not limited in this document.

4.1.1. Definition of HEADER Part

The HEADER part should include PRI,VERSION,TIMESTAMP,HOSTNAME,APP-NAME,PROCID and MSGID. The PRI field indicates the log type. The VERSION field denotes the version number of traceback log. The HOSTNAME field identifies the device that originally sent the syslog message. The TIMESTAMP field contains the timestamp of syslog generation. The NAT device that generates the timestamp MUST use the NTP protocol, to synchronize with other devices in the network. The APP-NAME field identifies the device name that originated the log message. The PROCID field is used to provide the log group which the log belongs to. One log group indicates a group of operations interrelated with each other, e.g., creating a translation table for one session and removing this table. The MSGID field identifies the type of the log messgae. The PRI,TIMESTAMP,HOSTNAME and MSGID are mandatory fields, and the APP-NAME, PROCID are optional fields.

4.1.1.1. PRI

The PRI field is composed of Facility and Severity values. The algorithm of PRI is defined as: PRI = Facility*8+Severity. The definition of syslog function code (Facility) is shown in Figure 2.

Code Value	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslog
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

Figure 2: Definition of Facility

In this document, the Facility value is denoted to be 16.

The definition of syslog severity code (Severity) is shown in Figure 3.

Code Value	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

Figure 3: Definition of Severity

In this document, the Severity value is denoted to be 6.

4.1.1.2. VERSION

The VERSION filed is set to 1.

4.1.1.3. TIMESTAMP

The format of TIMESTAMP is as below:

< year> < mon> < day> < hh:mm:ss>

year indicates the year the operation happens, which must be four digits, e.g., "2012". mon indicates month, and it could be one of the following values:Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov and Dec. day denotes the date, from 1 to 31. Hh, mm and ss separately denote the hours, minutes and seconds.

4.1.1.4. HOSTNAME

The HOSTNAME field identifies the IPv4 address of the originating device, which is in the format of the dotted decimal notation, e.g., 10.1.1.1.

4.1.1.5. APP-NAME

The APP-NAME field identifies the name of the device that originated the syslog message. It could be configured to the device by the manager, denoting the type of device, deployment site and model.

4.1.1.6. PROCID

The PROCID field is used to provide the number for a log group (the length of the number is suggested to be 16 bytes), which includes digits and characters. It identifies the interrelated logs in one device. The PROCID is allocated sequencely to the log group and could be used repeatedly for the next allocation.

4.1.1.7. MSGID

The MSGID field identifies the type of the message. The format is defined as: < device type>: < message type>. In the NAT444 environment, the device type is NAT444. In the DS-Lite environment, the device type is DSLITE. The message type in MSGID includes:

- UserbasedA:this message is for user based log allocation.

- SessionbasedA:this message is for session based log allocation.

- UserbasedW:this message is for user based log withdrawal.

- SessionbasedW:this message is for session based log withdrawal.

For example, the MSGID of user based log allocation for a DS-Lite device is:DSLITE:userbasedA.

4.1.2. Definition of MSG Part

The MSG part uses the ASCII characters. It MUST include the following contents:

- L4 application identification:1 indicates ICMP; 6 indicates TCP and 17 indicates UDP.

- Original Source IP:Source IPv4 address before translation.

- Original Source IPv6:Source IPv6 address before translation.

- Translated Source IP:Source IPv4 address after translation.

- Original Port:Source port before translation.

- Translated First Source Port:The first source port after translation, or source port after translation in session based translation.

- Translated Last Source Port:The last source port after translation.

The format of MSG part is:[<L4> < Original Source IP > < Original Source IPv6> < Translated Source IP > < Original Port > < Translated First Source Port > < Translated Last Source Port >]. for the parameters not existed in certain type of devices, the "-" is used.

Two examples:

1. Session based UDP port mapping allocation in NAT444 case:[17 10.0.0.1 - 192.168.0.1 - 10000 11000].

2. Session based TCP port mapping allocation in DS-Lite case:[6 - 2001::1 192.168.1.1 80 80 -].

4.1.3. Examples

The following is an example of the syslog log message for user based UDP allocation in NAT444 case: < 134> 1 2012 Jun 7 12:34:08 10.1.1.1 nat444-jiangsu - NAT444:userbasedA [17 10.0.0.1 - 192.168.0.1 - 10000

11000].

4.2. The Radius Interface Requirements

The radius interface should use the Raidus message format defined in [RFC2865] or [RFC2866]. for the first traceback solution introduced above, there is no change to the radius interface. The syslog message format is shown in section 4.1. for the solution 2, the traceback information is carried in the radius Accounting-Request packet. The attributes are extended as below:

Sub-Attr Name	Sub-Attr Number	Maximum Length	Type	Description	Notes
Vendor Extension:Vendor-ID is owned by each vendor					
USER-ESS-TYPE	120	4	Integer	Indicates users access address type	0-Public IPv4 user; 1-Private IPv4 user; 2-Public DS user; 3-Private DS user; 4-DS-Lite user; 5-Pure IPv6 user
USER-ESS-LOG	121	253	String	Stores various log information of NAT translation	This field contains mapping time, public address,original port, destination port, user address, each separated by ":". Example: mapping time (YY/MM/DD/HH/MM/SS); public address (IPv4); user address (IPv4 or IPv6)

Figure 4: Attributes Extension

For the radius server, USER-ADDRESS-TYPE attribute should be carried in the Accounting-Response message.

For the BRAS side: Vendor-ID is owned by each vendor. The sub-attr name, sub-attr number and type could be defined by the vendor itself. In the solution 2, the private attributes reported should be the translated address and ports(source and destination).

In the traceback solution 3, NAT device reports the dynamic user

address/port mapping information to the log server using Radius message.

For the radius server, USER-ADDRESS-TYPE attribute should be carried in the Accounting-Response message.

For the BRAS side: Vendor-ID is owned by each vendor. The sub-attr name, sub-attr number and type could be defined by the vendor itself.

BRAS reports the user traceback information to AAA server, in a delayed fixed time after sending the Accounting-Request message. Or BARS sends the information to other ports of the AAA server for which to collect the traceback information. In the solution 3, the private attributes reported should be the user account, mapping time, private address before translation, translated public address and ports(source and destination).

5. The Performance Requirements of The Log Server

There are some requirements for the log server:

- The packet processing capability of a single log server to receive syslog packet should not be less than 1,000 packets per second (CPU occupation rate should not exceed 50%).
- The response time of a single log server to process syslog packet should be less than or equal to 10 ms.
- The packet processing capability of a single log server to process log packet using Radius message should not be less than 1,000 packets per second (CPU occupation rate should not exceed 50%)
- The response time of a single log server to process the log packet using Radius should be less than or equal to 10 ms.
- The log should be stored in the storage system of the log server for 6 months.

6. The Reliability Requirements of The Log Server

The requirements of reliability is listed as below:

- The system should meet or exceed 99.999% usability.
- The continuous work time without failure should be more than 100 thousand hours.

- The failure recovery time should be less than 30 minutes.
- High reliability and stability. Main processor, main cache, power and management interface should have hot standby capability.
- The server should have 1:1 backup.
- The blade system should support hot plug and pull.

7. IANA Considerations

No request to IANA.

8. Security Considerations

None.

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC3195] New, D. and M. Rose, "Reliable Delivery for syslog", RFC 3195, November 2001.

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, March 2009.

[RFC5425] Miao, F., Ma, Y., and J. Salowey, "Transport Layer Security (TLS) Transport Mapping for Syslog", RFC 5425, March 2009.

[RFC5426] Okmianski, A., "Transmission of Syslog Messages over UDP", RFC 5426, March 2009.

Authors' Addresses

Zhonghua Chen
China Telecom
P.R. China

Phone:
Email: 18918588897@189.cn

Cathy Zhou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Phone:
Email: cathy.zhou@huawei.com

Tina Tsou
Huawei Technologies (USA)
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4424
Email: tina.tsou.zouting@huawei.com