Internet Draft <<u>draft-bakke-dhc-snmp-trap-01.txt</u>> Standards Track Expires May 2003

November 2002

DHCP Option for SNMP Notifications

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of <u>Section 10 of RFC2026</u>.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/lid-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

The Dynamic Host Configuration Protocol [RFC1531] provides a method for a host to retrieve common configuration parameters at boot time. These include the host's IP address, default gateway, subnet mask, DNS server, and other useful things.

When a host is booted from the network, it does not have access to these configuration parameters from its local or network disk right away; it relies instead on DHCP to provide them. One such parameter that is not yet provided is a list of IP hosts to which to send SNMP

Bakke

Expires May 2003

[Page 1]

Internet Draft DHCP Option for SNMP Notifications November 2002

notifications [RFC1448] during the boot process, particularly if the boot fails. As the host is already gleaning similar information from DHCP, a new option to specify these SNMP "trap" hosts appears to be the simplest method to gain this information. Hosts not booting from the network benefit as well, since SNMP notification hosts can now be configured centrally through DHCP.

There are an increasing number of solutions that allow hosts, racks of servers and embedded devices to be booted from the network. Many of these solutions include 10s, 100s, or 1000s of identical thin servers or blade servers which need to be monitored and managed centrally. When a network boot fails, there is currently no standard method to configure destinations to which to send SNMP notifications, allowing corrective action to be taken.

This document describes a proposed DHCP option that specifies a list of SNMP notification targets to which SNMP notifications should be sent.

Acknowledgements

This draft was produced as a result of discussions with Keith McCloghrie. Thanks also to David Harrington, Bert Wijnen, and Ira McDonald for pointing out the (many) holes in the first version.

1. 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 [RFC2119].

2. DHCP Option

The snmp-notification-list option is a UTF-8 string consisting of a comma-separated list of SNMP notification targets. SNMP notification hosts SHOULD be listed in order of preference; an implementation SHOULD send each notification to as many of the hosts listed as possible.

Each target is a set of parameters, separated by the ASCII colon character (':' = U+003a), which must appear in the following order:

 processor-model is a literal ASCII string which specifies one of the message processing model values defined in [<u>RFC2751</u>] in the SnmpMessageProcessingModel TC:

Expires May 2003

[Page 2]

v1 - SNMPv1 v2c - SNMPv2c v3 - SNMPv3

This field must not be left blank.

- ip-address is specified as either a dotted-decimal IPv4 address, a bracketed hexadecimal IPv6 address, or a DNS host name. This field must not be left blank. Examples are:

10.1.50.100 [1080:0:0:0:8:800:200C:417A] mytraphost.example.com

Note although the IPv6 format contains the colon character also used as a field separator, the bracketed notation keeps the two from being confused.

- udp-port is a decimal field containing the target UDP port. If left blank, the default UDP port is 162.
- security-model is a literal ASCII string which specifies one of the security models defined in [RFC2571] in the SnmpSecurityModel TC:

v1 - SNMPv1 v2c - SNMPv2c usm - User-Based Security Model

If the security-model field is left blank, no security is used.

The security-model field determines the format of the remainder of the notification target string. If the security-model is v1 or v2c, the next (optional) field is the community string:

- community-string specifies the community string to use when sending notifications to the target. If not specified, the default is "public".

If the security-model is "usm", two additional fields are required:

- security-level - This is the decimal security level number as specified in [RFC2571] in the SnmpSecurityLevel TC:

noAuthNoPriv - No authentication, no privacy authNoPriv - Authentication, with no privacy authPriv - Authentication and privacy

Expires May 2003

[Page 3]

This field MUST be specified when using the user-based security model.

- security-name - This is the UTF-8 security name to be used with notifications to this target.

3. Examples

A group of two v3 targets, both using USM with authentication but no privacy:

v3:128.1.2.3:162:usm:authNoPriv:joe, v3:128.2.4.6:162:usm:authNoPriv:joe

(carriage return inserted for clarity)

A single v3 target, using USM with both authentication and privacy:

v3:128.1.5.9:162:usm:authPriv:bob

A single address that wants both v1 and v2c notifications with the default community string and UDP port:

v1:10.1.1.1,v2c:10.1.1.1

An SNMPv2 address that uses a different community string:

v2c:10.50.2.100:my-community

4. Using Security Names

When using security names with the User-based Security Model, it is assumed that each of the referenced security names has been configured with its proper credentials, and can be used when sending notifications. However, this may not always be true. When booting the host from a network device, the configuration information for these credentials is normally stored on the network device, in a registry or configuration file. Events that cause notifications can happen after receiving the snmp-notification-list DHCP option, and before this configuration information is read from the device. When sending an SNMPv3 notification using the user-based security model (USM), these rules should be followed:

- If the security-level is "noAuthNoPriv", the security-name is not necessary; send the notification as normal.

Expires May 2003

[Page 4]

- If the security-level is "authNoPriv", send the notification without authentication as if it were "noAuthNoPriv". In this case, it's probably better to send the alert unauthenticated than not at all.
- If the security-level is "authPriv", do not send the notification.

5. Security Considerations

DHCP is normally deployed using authentication or security mechanisms. Authentication is available using [<u>RFC3118</u>].

Potential exposures to attack when authentication is not being used are discussed in <u>section 7</u> of the DHCP protocol specification [<u>RFC2131</u>]. Exposures when authentication is being used is described in [<u>RFC3118</u>].

6. IANA Considerations

IANA is requested to allocate a DHCP option number for this option.

7. Summary

This document describes a DHCP option for configuring a list of SNMP notification targets.

8. Normative References

- [RFC2026] S. Bradner, "The Internet Standards Process", <u>RFC 2026</u>, October 1996.
- [RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", <u>RFC 2119</u>, March 1997.
- [RFC2131] R. Droms, "Dynamic Host Configuration Protocol", <u>RFC 2131</u>, March 1997.
- [RFC1905] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Protocol Operations for SNMPv2", <u>RFC 1905</u>, January 1996.
- [RFC2571] D. Harrington, R. Presuhn, B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", <u>RFC 2571</u>, April 1999.

Expires May 2003

[Page 5]

DHCP Option for SNMP Notifications November 2002 Internet Draft

9. Informative References

- [RFC2132] S. Alexander, R. Droms, "DHCP Options and BOOTP Vendor Extensions", <u>RFC 2132</u>, March 1997.
- R. Droms, "Procedures and IANA Guidelines for Definition of [RFC2939] New DHCP Options and Message Types", <u>RFC 2939</u>, September 2000.
- R. Droms, W. Arbaugh, "Authentication for DHCP Messages", [RFC3118] RFC 3118, June 2001.

Author Contact Information

Mark Bakke Cisco Systems, Inc. 6450 Wedgwood Road Maple Grove, MN USA 55311

Voice: +1 763-398-1000 E-Mail: mbakke@cisco.com

10. Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING

Expires May 2003

[Page 6]

TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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