WebDHCP Technical Documentation

Table of Contents

1. Introduction

Webdhcpd is an application that uses encryption, logging, and documentation to add, delete, and modify entries in the DHCP config file. Please note that this program assumes the following:

- perl is installed in '/usr/bin/perl'
- DHCPD leases and config files are in '/etc'
- you are running ISC DHCPD v. 2.0pl5 or lower. The latest version has not been tested yet.

I have tested this program under Red−Hat Linux 6.2 − 7.0 and Solaris 7−8. There should not be any issues related to other versions of UNIX except for directory locations. I will continue to improve scripts to detect the proper locations of these files so that you will not have to modify any variables in the perl scripts.

Because of lack of time, the 'webdhcp_client.cgi' file has all of the html code imbedded in it. Please feel free to modify this code to suite your environment. If you would like to contribute a template mechanism, I will gladly incorporate it into this distribution and give you credit when a revision is released.

1.1. Requirements

1. ISC's DHCP server (www.isc.org)
2. UNIX (Tested on Solaris 8 & Red−hat Linux 6.0−7)
3. Perl 5.6.0
4. Apache 1.3.12
5. Perl Encryption Modules (www.cpan.org)
    - Crypt−Blowfish−2.06
    - Crypt−CBC−1.25
    - Crypt−CBCeasy−0.21
    - MD5−1.7

2. How does this thing work?

I originally thought about writting this program as the DNS/DHCP administrator at Kennesaw State. There were a few administrators in different departments that routinely needed me to manually add/delete entries in the DHCP database. It was simply too time consuming on my part to probe through the *dhcpd.conf* file to modify all requested entries and to a kill −HUP on the DHCPD daemon.

The security needed for this automated process needed to be tight. Ideally:

1. The administrator logs in through an SSL enabled browser
2. The web server authenticates the user via Apache
3. The web server checks *local documentation* to determine the next free IP address. This would be based on the subnet chosen
4. The web server also logs vi syslog the username of the administrator as well as what task they perform
5. Next, the client (web server) sends the server (WebDHCP daemon) an encrypted string representing the requested action
6. The WebDHCP daemon varifies that the data is both encrypted with the correct key and that it is coming from an allowed IP address. (I know, IP Spoofing comes to mind, but the key must be known in order to decrypt the request)
7. Assuming that the above conditions are met, WebDCHP will process the request and send back the results in the form of an encrypted string to the client (Web Server). Finally, the web server decrypts the results and displays it to the administrator via the web browser.

Note: The term *local documentation* assumes that you have clear text files on the web server with documented reserved IPs. This feature will be optional in future releases.

---

3. Why have so many files?

Here is the description of key files found in this distribution:

Files Location

File	***Description***
init.webdhcpd	init script, this is the recommended method of starting and stopping the server
webdhcpd_server	webdhcpd deamon, written in perl. Listens for requests via a specified port. This file Should be SUID root.
Webdhcp_Server.pm	Perl Module which interacts directly with the DHCP leases and configuration files
Webdhcp_Client.pm	Perl Module which does encryption and connects to the server
webdhcp_client.cgi	Cgi based client. Customized to used 'subnet.x' files as bases of IP availability. This file should also be SUID root
webdhcp_client.conf	Variable definitions for the client
subnet_example.doc	This is a sample file that was used to determine if an IP address is free or not. This piece could easily be rewritten to suite your environment.

4. Credits

Person	***Description***
Thomas Akin	helped with the encryption on the backend
Borek Lupomesky	who's "dhcplst.pl" program provided me with the idea of storing DHCP objects into hashes

5. Screenshots

- Screenshot 1
- Screenshot 2
- Screenshot 3
- Screenshot 4
- Screenshot 5

6. Where do I get this program?

- The latest copy could be found here.

Sourceforge

Last Modified: 19 May 2001.