Paquetage HTTPD - Serveur Web pour afficher le statut
Version 3.10.19

Frank Meyer
courriel: frank@fli4l.de

L'équipe fli4l
courriel: team@fli4l.de

2 février 2020

Table des matières

1. Documentation du paquetage HTTPD

1.1. HTTPD - Statut du routeur avec le serveur web

1.1.1. OPT_HTTPD - Mini serveur web comme moniteur de statut

Pour ceux qui n'ont pas la possibilité d'utiliser IMONC, pour certaines raison, par ex. parce qu'il utilise un Mac, ils peuvent utiliser le serveur web pour obtenir ou modifier le statut du routeur fli4l. En activant la variable `OPT_HTTPD='yes'`, vous pouvez utiliser le serveur web et l'écran du statut fli4l.

Pour obtenir la page d'accueil du statut, il faut indiquer dans votre navigateur l'une des adresses suivantes :

```
http://fli4l/
http://fli4l.domain.lan/
http://192.168.6.1/
```

Si votre routeur fli4l a un nom différent, celui-ci doit être utilisé à la place de "fli4l". Cela vaut aussi pour le nom de domaine et aussi pour l'adresse IP. Si vous avez configuré le serveur web sur un autre port (avec la variable `HTTPD_PORT`), vous devez indiquer ceux-ci :

```
http://fli4l:81/
```

Depuis la version 2.1.12 vous pouvez accéder à une page d'accueil pour le login et le mot de passe. Si vous voulez aller directement sur la page d'authentification avec le mot de passe et le login, cette page se trouve dans le sous-répertoire admin et vous devez spécifier alors :

```
http://fli4l.domain.lan/admin/
```

Vous pouvez configurer le serveur web avec les variables suivantes :

HTTPD_GUI_LANG Vous pouvez régler avec cette variable la langue, dans laquelle l'interface web doit être affichée. Si vous enregistrez 'auto', le réglage linguistique de la variable `LOCALE` (dans base.txt) sera utilisé.

HTTPD_LISTENIP Normalement, le serveur web se connecte sur une adresse Wildcard (ou adresse pouvant prendre n'importe quelle valeur), de sorte qu'il puisse réagir sur n'importe quelle interface du routeur. On peut aussi connecter une seule adresse IP, cela peut être paramétré dans cette variable. Pour l'enregistrement d'une seul adresse IP il faut qu'elle soit indiquée dans : `IP_NET_x_IPADDR`. Normalement, le réglage de la variable doit rester vide, pour que la valeur par défaut puisse fonctionner (sur n'importe quel adresse IP réactif).

Ce paramètre sert uniquement pour le httpd, il est associé seulement à une adresse IP, il ne peut pas être utilisé, pour accéder aux différents sous-réseaux de l'interface Web du routeur, car les accès seront bloqués. Si vous voulez utiliser d'autres adresses IP dans

cette variable, vous devez utiliser le filtrage de paquets, pour que l'ensemble des adresses soient reconnus sur le routeur. Il est possible d'indiquer plusieurs adresses IP, en les séparant par un espace.

HTTPD_PORT Si le serveur web doit fonctionner sur un autre port que 80, cette variable doit être adaptée. Normalement cela n'est pas très recommandé, car nous devons alors interroger le serveur web avec http ://fli4l :81/

HTTPD_PORTFW Si l'on met cette variable sur 'yes', on peut effectuer des changements sur la transmission de port par l'intermédiaire de l'interface de web. Les règles peuvent être supprimées ou ajoutées, ces modifications entrent en vigueur immédiatement. Mais ces modifications ne sont valable que pour la durée de fonctionnement du routeur. Si le routeur est redémarré, les modifications sont annulées.

Paramètre par défaut 'yes'.

HTTPD_ARPING Le serveur web montre l'état des hôtes en-ligne, ceux-ci sont énumérés dans la variable `HOST_x`. Le serveur utilise le *"cache-arp"*, pour enregistrer provisoirement dans la mémoire les adresses des hôtes locaux. Si un ordinateur n'a pas communiqué depuis longtemps avec le routeur, son adresse IP disparaît du *"cache-arp"* et l'hôte semble être déconnecté. Vous devez tenir à jour le *"cache-arp"* (cela empêchera les hotes qui ne sont pas réellement déconnectés de ne plus être vu), pour cela vous devez activer la variable `HTTPD_ARPING` et mettre la valeur *'yes'*.

HTTPD_ARPING_IGNORE_N Dans cette variable vous enregistrez le nombre de arping qui seront ignoré.

HTTPD_ARPING_IGNORE_x Dans cette variable vous indiquez l'adresse IP ou nom de l'hôte qui ne sera pas inclus dans le test arping. Cela peut être utile, pour les hôtes qui utilisent (le wifi du réseau local pour les ordinateurs portables ou les téléphones). Car les paquets de requêtes régulières passant par le réseau consomment plus rapidement la batterie.

1.1.2. Gestion des utilisateurs

Le serveur web offre à utilisateur une administration précise :

HTTPD_USER_N Avec cette variable on ajuste, le nombre d'utilisateurs. Si cette variable est placée sur 0, l'administration des utilisateurs est désactivée complètement et tous le monde a la possibilité d'interroger le serveur web.

HTTPD_USER_x_USERNAME HTTPD_USER_x_PASSWORD HTTPD_USER_x_RIGHTS Avec ces variables on paramètre les différents utilisateurs avec, le nom d'utilisateur, le mot de passe et les droits. On règle Dans la variable `HTTPD_RIGHTS_x` les fonctions pour que chaque utilisateur puisse interroger le serveur web. Dans le cas le plus simple, on paramètre seulement 'all' ce qui signifie que l'utilisateur correspondant peut interroger toutes les fonctions. La variable peut avoir les constructions suivantes :

```
'fontion1:droit1,droit2,... fonction2:...'
```

Au lieu d'indiquer les différents droits pour chaque fonction, la valeur "all" peut être paramétrée, ainsi l'utilisateur aura tous les droits pour chaque fonction. Ci-dessous les fonctions et droit :

Fonction "status" Tout ce qui peut être vue dans le menu statut

view L'utilisateur peut lancer tous les points du menu.

dial L'utilisateur peut décrocher et raccrocher la ligne Tél.

boot L'utilisateur peut arrêter & redémarrer le routeur.

link L'utilisateur peut ajouter ou mettre hors circuit un canal (ISDN)

circuit L'utilisateur peut changer le circuit.

dialmode L'utilisateur peut modifier le mode-dial (Auto, Manual, Off).

conntrack L'utilisateur peut voir les connexions actuelles en fonctionnent sur le Routeur.

dyndns L'utilisateur peut voir les informations du paquetage `DYNDNS` (Page **??**).

Fonction "logs" Tout se que l'on peut faire avec le fichier log (ou fichier journal) (connexion, appels, Syslog)

view L'utilisateur peut voir le fichier journal des événements.

reset L'utilisateur peut supprimer le fichiers journal des événements.

Fonction "support" Tout ce qui est utile, pour chercher des informations par exemple de l'aide dans le Newsgroup.

view L'utilisateur peut utiliser les liens pour la documentation, aller sur à la page Web de fli4l, etc.

systeminfo L'utilisateur peut voir les informations sur la configuration et l'état actuel du routeur (par ex. le pare-feu).

Voici quelques exemples :

HTTPD_USER_1_RIGHTS='all' Avec ce paramètre l'utilisateur peut tous faire !

HTTPD_USER_2_RIGHTS='status :view logs :view support :all' Avec ces paramètres l'utilisateur peut tout voir, mais rien modifier.

HTTPD_USER_3_RIGHTS='status :view,dial,link' Avec ces paramètres l'utilisateur peut suivre l'état de la connexion Internet, choisir l'agrégation des canaux (ISDN) ou de l'éteindre.

HTTPD_USER_4_RIGHTS='status :all' Avec ce paramètre l'utilisateur peut tout faire avec les connexions Internet, aussi de redémarrer (et naturellement arrêter le routeur). Cependant il ne peut pas voir le fichier journal ou de l'effacer, il ne peut pas non plus voir les plages horaires des connexions Internet...

1.1.3. OPT_OAC - Contrôle d'accès en ligne (OAC)

OPT_OAC (Variable optionnelle)

Avec cette variable vous activez le module pour le contrôle d'accès en ligne (OAC), l'accès Internet peut être configuré par rapport aux clients, sélectionnable dans le paquetage dns_dhcp (Page **??**), ainsi les ordinateurs auront une mobilité réduite.

Cet outil existe également en ligne de commande, il permet de contrôler d'autres paquets, par ex. Easycron :

/usr/local/bin/oac.sh

Les options sont affichées avec la commande ci-dessous.

OAC_WANDEVICE (Variable optionnelle)

Avec cette variable vous indiquez le périphérique réseau qui sera utilisé pour restreindre ou verrouiller les accés. Par ex. 'pppoe'

OAC_INPUT (Variable optionnelle)

Avec cette variable vous assurez la protection contre l'environnement via le Proxy.

OAC_INPUT='default' bloque les ports des configurations de : Privoxy, Squid, Tor, SS5, Transproxy.

OAC_INPUT='tcp :8080 tcp :3128' bloque le Port TCP 8080 et 3128. Ici on bloque une liste de Ports avec le protocole qu'il l'accompagne (UDP, TCP), les ports seront séparés par un espace. Si le protocole udp ou tcp n'est pas indiqué, le port ne sera pas conforme.

Vous pouvez omettre cette variable ou indiquer 'no' pour désactiver cette fonction.

OAC_ALL_INVISIBLE (Variable optionnelle)

Avec cette variable on passe sur la vue d'ensemble, pour savoir s'il existe au moins un profil de groupe visible. S'il n'y a pas de profil de groupe visible, alors cette variable n'a aucune action.

OAC_LIMITS (Variable optionnelle)

On indique dans cette variable une limite temps, que vous pouvez choisir dans la liste ci-dessous. Les limites temps sont donnés en minutes. De cette façon, vous pouvez bloquer ou le débloquer temporairement un accés sur le réseau.

Par défaut : '30 60 90 120 180 360 540'

OAC_MODE (Variable optionelle)

Dans cette variable les valeurs possibles sont : `'DROP'` ou `'REJECT'` (par défaut)

OAC_GROUP_N (Variable optionnelle)

Dans cette variable vous indiquez le nombre de groupes clients. Pour plus de clarté, vous pouvez également utiliser l'interface web pour créer l'ensemble des groupes, qui seront autoriser ou bloquer.

OAC_GROUP_x_NAME (Variable optionelle)

Avec cette variable vous indiquez le nom du groupe. Ce nom sera affiché dans l'interface web et sera également utilisable avec le script 'oac.sh' en ligne de commande.

OAC_GROUP_x_BOOTBLOCK (Variable optionnelle)

Si vous indiquez dans cette variable 'yes', tous les clients du groupe seront bloqués lors du boot. En règle générale ces ordinateurs seront verrouillés et pas seulement dans certains cas exceptionnels.

OAC_GROUP_x_INVISIBLE (Variable optionnelle)

Dans cette variable vous pouvez marquer le groupe comme invisible. Si ces ordinateurs sont bloqués à l'avance, ces groupes ne seront pas visibles dans l'interface web.

OAC_GROUP_x_CLIENT_N (Variable optionelle)

Dans cette variable vous indiquez le nombre de clients dans le groupe.

OAC_GROUP_x_CLIENT_x (Variable optionelle)

Dans cette variable vous indiquez le nom du client, qui est paramétré dans la variable `HOST_x_NAME` du paquetage dns_dhcp. (Page **??**)

OAC_BLOCK_UNKNOWN_IF_x (Variable optionelle)

Dans cette variable vous indiquez la liste des interfaces définies dans le fichier base.txt, sur lesquels, seuls les hôtes définis dans le fichier (dns_dhcp.txt) pourront accéder à Internet. Les hôtes non définis seront généralement bloqués.

A. Annexe du paquetage HTTPD

A.1. HTTPD

A.1.1. Paramètre supplémentaire

Normalement ces paramètres ne se trouvent pas dans le fichier de configuration, ils doivent être ajoutés si nécessaires.

HTTPD_USER Avec cette option, il est possible de faire fonctionner le serveur-Web avec les droits d'un autre utilisateur, en tant "root". Ceci est particulièrement utile, lorsque le serveur-Web est utilisé pour mettre à disposition d'autres pages que l'interface d'Admin. Attention : Il est possible que certains Scripts ne fonctionnent plus, car ils ont besoin d'accéder à certains fichiers de configuration. Le scripts par défaut de ce paquetage, fonctionne pour chaque utilisateur.

A.1.2. Observation générale

Si vous avez installé TELMOND, dans la fonction statut sur la page call de l'interface-Web, se trouve les numéros de téléphones des correspondants. Un classement par nom peut être fait dans le fichier opt/etc/phonebook. Ce fichier a le même format que le fichier des numéros de téléphone d'IMONC. Ces annuaires téléphoniques peuvent être échangés entre IMONC et le routeur. Le format de chaque ligne du fichier est le suivant "Telefonnummer=Name [,fichier-WAV]" (sans les guillemets). Cependant le fichier WAV est utilisé uniquement par IMONC il est ignoré par le serveur-Web.

Le design des pages de l'interface-Web a été complètement remanié depuis la version 2.1.12 avec le fichier CSS. Les vieux navigateurs web pourraient avoir des problèmes avec cette version. Cette version a l'avantage, de pouvoir changer à volonté l'aspect de l'interface web, il suffit simplement d'adapter le fichier CSS (essentiellement le fichier /opt/srv/www/css/main.css).

Le paquetage serveur-Web a été produit par Thorsten Pohlmann (courriel: pohlmann@tetronik.com) et est maintenu à présent par Tobias Gruetzmacher (courriel: fli4l@portfolio16.de). La nouvelle conception (voir version 2.1.12) a été réalisée par Hummel Helmut (courriel: hh@fli4l.de).

Table des figures

Liste des tableaux

Index