Linux server

KKK-LIN

Szerver telepítése és beállításai

A Linux szervereinken a Debian 12.7-es verzióját használjuk, és grafikus felület nélküli telepítést végzünk, mivel a konfigurációs feladatokhoz nincs szükség GUI-ra és így jobb lesz a szerver erőforráskihasználása. A telepítés során megadott értékeket az *x-y. képeken* láthatják.

|  |
| --- |
| *x. kép - Hosztnév* |
| *x. kép – Domain név* |
| *x. kép – Alap csomagok* |

A következő (*x. kép*) képen a szerver IP beállításai tekinthetők meg:

|  |
| --- |
| *x. kép – IP beállítások* |

A szerverre pár egyéb csomagot is telepítettünk, ami még a szerver alapvető kezeléséhez szükséges. Ezek a(z):

* mc (GUI-s fájlkezelő)
* dnsutils (DNS lekérdezésekhez szükséges parancsok)
* net-tools (IP cím, interfész konfigurációs beállítások)
* ldap-utils (LDAP lekérdezések a Windows szerverről)

Ansible

Mivel a fő Windows szervereink függősége a Ansible playbookok megléte és futtatása, ezért első sorban ezt a környezetet hoztuk létre. A következő csomagokat telepítettük ehhez:

* ansible
* ansible-core

A hálózati automatizáció részben tovább olvashatnak ezekről a megoldásokról, valamint a hivatkozásoknál megtekinthetik a megírt kódokat.

LibreNMS

A LibreNMS egy olyan szolgáltatás, ami egyszerre nyújt Syslog, SNMP és egyéb hálózat monitorozó lehetőségeket. A sokoldalúsága miatt döntöttünk a szolgáltatás mellett, amik segítenek a hálózat későbbi esetleges hibáinak, gyengülésének, és ezeknek a gócpontoknak a felderítésében. A szolgáltatás komplex konfigurációjátnak telepítését a GitHub repozitóriumában leírt dokumentációja alapján végeztük el.

**A szolgáltatás telepítése (CÍM)**

A LibreNMS szolgáltatás futtatásra a Docker konténert használjuk a jobb erőforráskihasználás érdekében. Ennek a telepítését a Docker oldalán található dokumentáció alapján végeztük el (<https://docs.docker.com/engine/install/debian>).

Miután feltelepítettük a Docker-t a szervergépünkre, a DockerHub-ból átirányítva a GitHub oldalon lévő dokumentáció alapján telepítettük a szolgáltatást. (<https://github.com/librenms/docker>). A telepítés során a következő lépéseken keresztül haladtunk végig:

* *cp examples/compose /var/librenms/* (átmásoljuk a példa fájlokat)
* A saját változóinkra kicseréltük a \*.env -re végződő fájlok hiányos beállításait, amelyeket a következő képeken láthatóak (*x-y. kép*): 3 kép beszúrása
* *docker compose up -d* (futtatom a beállításaim alapján a LibreNMS szolgáltatást)

|  |
| --- |
| *x. kép - .env fájl* |
| *x. kép – librenms.env fájl* |
| *x. kép – msmtpd.env fájl* |

**A szolgáltatás tesztelése (CÍM)**

A szervereket a SNMPv2c segítségével adtuk hozzá a felderítéshez, valamint beállítottuk, hogy a logjaikat küldjék tovább erre a szerverre. Az előre megadott „kulcs”, azaz a community name *KKK-SNMP*. A felvett szervereket a LibreNMS webfelületén a *x. képen* láthatják.

|  |
| --- |
| *x. kép – Szerverek listája SNMP-ben* |

A hálózati eszközök SNMPv3 segítségével, még biztonságosabban csatlakoznak SHA-512, és AES-256-C titkosítástok segítségével, valamint minden 6-os vagy annál súlyosabb szintű logot, elküldenek a szervernek. A felvett hálózati eszközöket a LibreNMS webfelületén a *x. képen* láthatják.

|  |
| --- |
| *x. kép – Hálózati eszközök listája SNMP-ben* |

Az eszközöket külön szerveztük, minden eszközt a saját locationjába, így adott siteok, eszközeit is képesek vagyunk egy felület alól megnézni, hogy minden rendben van-e velük, és hogy éppen milyen teljesítménnyel működnek, ha szükségünk lenne erre, valamint különböző szolgáltatásokat is megtekinthetünk.

Webszerver

A hálózatunkban a webszerver szolgáltatást arra használjuk, hogy Python segítségével, konfigurációkat tudjunk küldeni SSH-n keresztül adott eszközöknek, egy konfiguráció összerakását segítő oldalon. A weboldal alapvetően kisebb kártyákból épül fel, ami mellett megtalálható az éppen beírt kód, a navbarban megadhatjuk, hogy milyen IPv4 címre, milyen felhasználóval és jelszóval küldjük az adatokat.

A weboldal egy Python script segítségével valósítja meg az SSH kapcsolatot, majd küldi el ezeket az adatokat a megadott SSH szervernek, amin végrehajtja, majd egy kimenetet ad a weboldal aljára, amin látható, hogy mi történ a parancssorban, a feladatok elvégzése közben, ha esetleg, valami elgépelés történt volna.

Az oldalt csak az IT csoport tagjai, használhatják, ezt egy LDAP-os bejelentkezéssel biztosítjuk. A webszerver kiszolgálja a klienseket, IPv4-gyel és IPv6-tal is.

**A szolgáltatás telepítése (CÍM)**

A következő szolgáltatásokat telepítettük fel ennek a megoldásnak a részeként:

* python3-pip, python3-venv, python3-flask, python3-paramiko
* apache2, libapache2-mod-wsgi-py3, libnss-ldapd, libpam-ldapd

A python3-mal kezdődő csomagok, a python script megfelelő futásáért, míg a többi csomag az apache2 webszerver és annak bővített moduljaiért felel, ezek segítenek a Python kód használatában, illetve az LDAP autentikációban.

**A szolgáltatás konfigurációja (CÍM)**

A weboldal hostolásához, először is megszüntettük az alapoldal elérhetőségét (*a2dissite 000-default*), ezen kívül létrehoztuk az */etc/apache2/sites-available/ssh\_website.conf* fájlt, aminek a következő a tartalma:

<VirtualHost \*:443>

    ServerName python.kkk.com

    WSGIDaemonProcess ssh\_website python-path=/var/www/ssh\_website:/var/www/ssh\_website/venv/lib/python3.9/site-packages

    WSGIProcessGroup ssh\_website

    WSGIScriptAlias / /var/www/ssh\_website/ssh\_website.wsgi

    SSLEngine on

    SSLCertificateFile /cert/mail.crt

    SSLCertificateKeyFile /cert/mail.key

    SSLCertificateChainFile /cert/ca.crt

    <Location />

        AuthType Basic

        AuthName "Login with just IT users!"

        AuthBasicProvider ldap

        AuthLDAPURL "ldap://kkk-adds.kkk.com/OU=IT,OU=Felhasznalok,DC=kkk,DC=com?sAMAccountName?sub?(objectClass=person)"

        AuthLDAPBindDN "CN=Administrator,CN=Users,DC=kkk,DC=com"

        AuthLDAPBindPassword "Password123"

Require all denied

        Require ldap-group CN=IT,OU=Csoportok,OU=Felhasznalok,DC=kkk,DC=com

        Require valid-user

    </Location>

    <FilesMatch "\.(?:cgi|shtml|phtml|php)$">

        SSLOptions +StdEnvVars

    </FilesMatch>

    <Directory /usr/lib/cgi-bin>

        SSLOptions +StdEnvVars

    </Directory>

    <Directory /var/www/ssh\_website>

        Require all granted

    </Directory>

    Alias /static /var/www/ssh\_website/static

    <Directory /var/www/ssh\_website/static>

        Require all granted

    </Directory>

    ErrorLog ${APACHE\_LOG\_DIR}/ssh\_website\_error.log

    CustomLog ${APACHE\_LOG\_DIR}/ssh\_website\_access.log combined

</VirtualHost>

A weboldalt SSL/TLS titkosítással védjük, hogy csak HTTPS-en keresztül lehessen elérni, az ehhez használt fájlokat, később az email szerver konfigurálásánál olvashatnak részletesebben, ezek közül a fő tanúsítvány az Active Directoryban, GPO segítségével meg lett osztva a domain tagjaival, a *mail.crt, mail.key* fájl pedig a titkosítás folyamatához szükséges tanusítványok.

A <Location> tageken belül pedig az LDAP-on keresztüli hitelesítést állítottuk be úgy, hogy csak az IT csoport tagjai tudjanak bejelentkezni az oldalra, a felhasználónevük és jelszavuk segítségével, ezen kívül van még egy biztonsági szűrő, ami csak a cég privát IPv4-es és publikus IPv6-os tartományából engedi a belépést a felhasználóknak.

A következő lépésben engedélyeztük a weboldalt a *’a2ensite ssh\_website’* paranccsal, ami létrehozott egy szimbolikus linket a */etc/apache2/sites-available/ssh\_website.conf* fájlról a */etc/apache2/sites-enabled/* mappába, ezután pedig engedélyeztük a következő modokat, hogy működjenek a konfigurációs fájlban tárolt beállítások. A modok engedélyezésére használt parancs: *’a2enmod ssl ldap authnz\_ldap auth\_basic’*. Ezek után a */var/www/ssh\_website/* elérési útvonal alá odamásoltuk a weboldalt, és a mappán a következő biztonsági beállításokat végeztük el: *’chown -R www-data:www-data /var/www/ssh\_website/’* valamint *’chmod -R 750 /var/www/ssh\_website/’* amik segítségével az apache2 felhasználója minden fájlt rekurzívan el tud érni a megadott mappában, a csoportja pedig olvasási és áthaladási jogot kap minden objektumra.

Ezt követően újraindítottuk a szolgáltatást és hiba nélkül lefutott, a weboldal, a webszerver elérhetővé vált.

**A szolgáltatás tesztelése (CÍM)**

A weboldal eléréséről, bejelentkezésről, valamint az oldal használtaáról a következőben olvashatnak.

A webszerver egy autentikációt kér, az *x-y. képen* a kliens és szerveroldali belépést, illetve sikertelen belépést láthatják. Itt látható, hogy Kovács Gábor az IT csoport tagja sikeresen bejelentkezett és lekérte a weboldal tartalmát, viszont Hajnal Tímeának a vezető csoport tagja nem tudta lekérni a weboldalt, megtagadta a lekérést, és 401-es hibakódra, azaz Unauthorized-re futott a kérés.

|  |
| --- |
| *x. kép – Bejelentkezés Kovács Gábor felhasználóval kliens oldalról* |
| *x. kép – Bejelentkezés Kovács Gábor felhasználóval szerver oldalról* |
| *x. kép – Bejelentkezés Hajnal Tímea felhasználóval kliens oldalról* |
| *x. kép – Hiba a bejelentkezés hiányában* |
| *x. kép – Bejelentkezés Hajnal Tímea felhasználóval szerver oldalról* |

A *x-y. képeken* az látható, ahogy megadott IPv4 címre megadott felhasználóval, a weboldal elküldi a kódot, amit a jobb oldali textarea-ba írt a felhasználó, valamint a kimenetet ugyanehhez a folyamathoz.

|  |
| --- |
| *x. kép – Adatok megadása és küldés* |
| *x. kép – POST kérés kimenete* |

Az *x. képen* a webszolgáltatás folyamatának a futásának állapota látható.

|  |
| --- |
| *x. kép – Apache2 státusza* |

Email

A Kihagyhatatlan Kincsek Kiadó hálózatában helyet foglal egy email szerver, ami a belső emailezésre szolgál, hogy ne egy külső szolgáltatón keresztül kelljen ezt elvégezni, hanem belső hálózatból, AD-s bejelentkezéssel lehessen végezni, így az egyedi email szolgáltatás árát megspórolva, egy teljesen jól működő rendszer készült el.

Technikai oldalról megközelítve, a KKK-LIN szerveren van egy dovecot, és postfix szolgáltatás, ami a KKK-ADDS-ről, a Domain Controller szerverünkről végzi az LDAP lekéréseket.

Az email szolgáltatás úgy, mint ahogyan az egész hálózat Dual Stack azaz IPv4, és IPv6-os megoldást is alkalmaz, így elősegítve a későbbi átállást az IPv6-ra.

A konfiguráció során több hibába is belefutottunk, az Active Directoryba való LDAP-os bejelentkezés megvalósítása során.

**A szolgáltatás telepítése (CÍM)**

Az email szolgáltatáshoz a Postfix/Dovecot párost használjuk. A Postfix felel az üzenetek elküldéséért, ez az SMTP szerverünk. A Dovecot felel az üzenetek fogadásáért, és emailek lekérdezéséért. A következő csomagokat telepítettük a szolgáltatásokhoz:

* dovecot-core dovecot-imapd dovecot-ldap
* postfix postfix-ldap

**A szolgáltatás konfigurációja (CÍM)**

Mivel itt is törekedtünk a biztonságos beállításokra ezért, először létrehoztuk a hitelesítő fájlokat. Készítettünk egy CA-t, ehhez egy privát kulcsot, ami a CA privát kulcsa. Ezek segítségével kiállítottunk egy Certificatet a KKK-LIN.kkk.com (mail.kkk.com, python.kkk.com) számára egy tanusítványt (publikus certificatet, és privát kulcsot). A CA-t beimportáltam a Default Domain Policy-be így a domainen belüli számítógépek számára, ez egy megbízható szerver lesz. Ezeket a kulcsokat, mind a Postfix mind a Dovecot használja (valamint, mint a korábbiakban említettük az Apache2 webszerver is).

A Postfix konfigurációjához, a fő fájlt *(/etc/postfix/main.cf)* kellett szerkeszteni, amit a következőképpen végeztünk el:

smtpd\_banner = $myhostname ESMTP $mail\_name (Debian/GNU)

biff = no

# appending .domain is the MUA's job.

append\_dot\_mydomain = no

readme\_directory = no

# See http://www.postfix.org/COMPATIBILITY\_README.html -- default to 3.6 on

# fresh installs.

compatibility\_level = 3.6

# TLS parameters

smtpd\_tls\_cert\_file=/cert/mail.crt

smtpd\_tls\_key\_file=/cert/mail.key

smtpd\_tls\_CAfile=/cert/ca.crt

smtpd\_tls\_security\_level=encrypt

smtp\_tls\_CApath=/cert

smtp\_tls\_security\_level=may

smtp\_tls\_session\_cache\_database = btree:${data\_directory}/smtp\_scache

smtpd\_relay\_restrictions = permit\_mynetworks permit\_sasl\_authenticated defer\_unauth\_destination

myhostname = mail.kkk.com

alias\_maps = hash:/etc/aliases

alias\_database = hash:/etc/aliases

myorigin = /etc/mailname

mydestination = $myhostname, KKK-LIN.kkk.com, localhost.kkk.com, localhost

relayhost =

mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 [2001:db8:c1c1:abfa::]/64 10.0.0.0/8

mailbox\_size\_limit = 0

recipient\_delimiter = +

inet\_interfaces = all

inet\_protocols = all

mydomain = kkk.com

virtual\_mailbox\_domains = $mydomain

virtual\_alias\_maps = ldap:/etc/postfix/ldap/virtual\_alias\_maps

virtual\_mailbox\_base = /

virtual\_mailbox\_maps = ldap:/etc/postfix/ldap/virtual\_mailbox\_maps

virtual\_uid\_maps = ldap:/etc/postfix/ldap/virtual\_uid\_maps

virtual\_gid\_maps = ldap:/etc/postfix/ldap/virtual\_gid\_maps

smtpd\_sender\_login\_maps = ldap:/etc/postfix/ldap/smtpd\_sender\_login\_maps

smtpd\_sasl\_type = dovecot

smtpd\_sasl\_path = private/auth

smtpd\_sasl\_auth\_enable = yes

broken\_sasl\_auth\_clients = yes

# Logging is optional but can help A LOT with debugging

maillog\_file = /var/log/postfix.log

A következő beállításokat tárolja ez a fájl:

* TLS beállítások (használja az általunk előállított tanusítványokat, és kulcsokat)
* A szerver nevét, elérhetőségét (IP kommunikáció alapján és név alapján)
* Virtuális mapolásokat (későbbiekben bemutatott fájlok)
* Dovecot használata
* Log fájlok helye

A *main.cf* fájlban található virtuális mapolások, az LDAP lekéréseket szolgálják, a következőkben a 4 fájl-t tekinthetik meg. Mindegyik fájl eleje megegyezik, ezek azt állítják, be, hogy honnan, és milyen felhasználó segítségével kérjék le a beállításokat:

server\_host = kkk-adds.kkk.com:389

version = 3

bind = yes

bind\_dn = cn=Administrator,cn=Users,dc=kkk,dc=com

bind\_pw = Password123

search\_base = ou=Felhasznalok,dc=kkk,dc=com

scope = sub

*virtual\_alias\_maps:*

…

query\_filter = (|(sAMAccountName=%s)(sAMAccountName=%s))

result\_attribute = sAMAccountName

A keresés a sAMAccountName mező alapján keres és azt is adja vissza (felhasználónév).

*virtual\_mailbox\_maps:*

…

query\_filter = (|(sAMAccountName=%s)(userPrincipalName=%s))

result\_attribute = sAMAccountName

result\_format = /mailboxes/%s/

Az előbbiekben leírt keresés a megadott mezők alapján keres, a felhasználónév, illetve a teljes név alapján (felhasználónév@domain), és az emailek lerakási helyét adja vissza *(/mailboxes/felhasználónév)*.

*virtual\_uid\_maps:*

…

query\_filter = (|(sAMAccountName=%s)(userPrincipalName=%s))

result\_attribute = uid

Ez a keresés ugyanúgy, mint az előző kérés a felhasználónév és az email cím alapján szűr. Viszont az uid mezőt adja vissza.

*virtual\_gid\_maps:*

…

query\_filter = (|(sAMAccountName=%s)(userPrincipalName=%s))

result\_attribute = gidNumber

Ez a keresés ugyanúgy, mint az előző kérés a felhasználónév és az email cím alapján szűr. Viszont az gidNumber mezőt adja vissza, tehát a csoportot. Ez a csoport egy univerzális csoport, aminek a felhasználók email könyvtárára, van 7 joga, ezzel létre tudja hozni az emaileket a megadott helyre.

*smtpd\_sender\_login\_maps:*

…

query\_filter = (|(userPrincipalName=%s)(sAMAccountName=%s))

result\_attribute = sAMAccountName

Fordítva intézi a keresést, és a felhasználónevet adja vissza.

A konfiguráció során, ezeknek a mapoknak a beállítása okozta a legnagyobb problémát, mivel az Active Directoryban nem tároltunk le alapvetően homeDirectory, uid is gidNumber mező értéket, amiből az uid-re a Postfixnek, a maradékra, és az uidra ugyanúgy a Dovecotnak van szüksége. Ezek a mezők, viszont nem voltak helyettesíthetők unique nevekkel, mint például a sAMAccountName, ezért a létrehozás során egy növekvő számértéket, adtunk minden felhasználónak, amivel így tudja azonosítani a Dovecot is.

A Postfixnél még két beállítást végeztem el a */etc/postfix/master.cf* fileban:

# Choose one: enable submission for loopback clients only, or for any client.

#127.0.0.1:submission inet n - y - - smtpd

submission inet n - y - - smtpd

# -o syslog\_name=postfix/submission

-o smtpd\_tls\_security\_level=encrypt

# -o smtpd\_sasl\_auth\_enable=yes

-o smtpd\_tls\_auth\_only=yes

...

# Choose one: enable submissions for loopback clients only, or for any client.

#127.0.0.1:submissions inet n - y - - smtpd

submissions inet n - y - - smtpd

# -o syslog\_name=postfix/submissions

-o smtpd\_tls\_wrappermode=yes

# -o smtpd\_sasl\_auth\_enable=yes

A Dovecot konfigurációja sokkal több fájlból áll össze, ezért csak rövid kódrészleteket mutatunk, amit megváltoztattunk az alapbeállításokhoz képest.

*/etc/dovecot/conf.d/10-mail.conf:*

mail\_location = maildir:/mailboxes/%u

namespace inbox {

prefix =

location = maildir:/mailboxes/%u

inbox = yes

separator = /

}

namespace {

prefix = Sent/

separator = /

list = yes

subscriptions = yes

location = maildir:/mailboxes/%u/Sent

}

namespace {

location = maildir:/mailboxes/%u/Trash

separator = /

prefix = Trash/

list = yes

subscriptions = yes

}

namespace {

location = maildir:/mailboxes/%u/Drafts

separator = /

prefix = Drafts/

list = yes

subscriptions = yes

}

Ezek a beállítások az emailek elhelyezési és kiolvasási helyét határozzák meg. Meg van adva, hogy az emailek a */mailboxes/felhasználónév/* elérési útvonal alatt található és ezalatt van bejövő-, elküldött-, kuka- és piszkozat emailek.

*/etc/dovecot/conf.d/10-ssl.conf:*

##

## SSL settings

##

# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>

ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before

# dropping root privileges, so keep the key file unreadable by anyone but

# root. Included doc/mkcert.sh can be used to easily generate self-signed

# certificate, just make sure to update the domains in dovecot-openssl.cnf

ssl\_cert = </cert/mail.crt

ssl\_key = </cert/mail.key

Megadjuk a publikus kulcsot és certificatet, valamint megadjuk, hogy bekapcsolt a SSL/TLS titkosítás.

*/etc/dovecot/conf.d/10-auth.conf:*

disable\_plaintext\_auth = no

mail\_privileged\_group = dovecot

auth\_mechanisms = plain login

#!include auth-system.conf.ext

!include auth-ldap.conf.ext

A következő sorokkal a bejelentkezés beállításait változtattuk meg. Kikapcsoltuk a system alapú bejelentkezést, és engedélyeztük az LDAP konfigurációs fájlt.

*/etc/dovecot/dovecot-ldap.conf.ext:*

# LDAP URIs to use. You can use this instead of hosts list. Note that this

# setting isn't supported by all LDAP libraries.

uris = ldap://kkk-adds.kkk.com

dn = CN=Administrator,CN=Users,DC=kkk,DC=com

dnpass = Password123

auth\_bind = yes

base = OU=Felhasznalok,DC=kkk,DC=com

scope = subtree

user\_filter = (&(objectClass=person)(sAMAccountName=%u))

user\_attrs = uid=uid,gidNumber=gid,homeDirectory=home

pass\_filter = (&(objectClass=person)(sAMAccountName=%u))

pass\_attrs = uid=uid,userPassword=password

Ez a fájl tartalmazza, az

* LDAP szervert
* Összekötő felhasználót
* Az alapvető keresési tartományt
* A felhasználó szűrést és attribútumokat
* A jelszó szűrést, és attribútumokat.

A filter és az attribútumok meghatározása az Active Directory miatt nehézkes volt, viszont sikeresen megoldottuk.

*/etc/dovecot/conf.d/10-master.conf:*

service auth {

...

# Postfix smtp-auth

unix\_listener /var/spool/postfix/private/auth {

mode = 0666

user = postfix

group = postfix

}

}

A következő beállítás meghatározza, hogy a Postfix az email küldő szolgáltatásunk.

*/etc/dovecot/conf.d/10-logging.conf:*

log\_path = /var/log/dovecot.log

Ezzel a sorral pedig meghatározzuk, hogy egy külön fájlba gyüjtse a log bejegyzéseket a szolgáltatás.

**A szolgáltatás tesztelése (CÍM)**

A tesztelés során két felhasználót *hajnal.timea* és *kovacs.gabor* felhasználói fiók segítségével teszteltünk. A kliensek egy oda vissza Reply üzenetet küldenek egymásnak, amikről a képeket *x-y. képeken* láthatják. Ezt követően az *x-y. képen* az ezekhez tartozó főleg Postfix, de a lekérésről lévő Dovecot bejegyzést is láthatják.

|  |
| --- |
| *x. kép – Email fogadása* |
| *x. kép – Válaszemail* |
| *x. kép – Válaszemail fogadása* |
| *x. kép – Postfix log első email küldése* |
| *x. kép – Postfix log válaszemail küldése* |
| *x. kép – Dovecot log (bejelentkezés levelek lekérése)* |

Rsyslog szerver

A logok összegüjtésére a hálózatban, amit nem tud befogadni a LibreNMS készítettünk egy Rsyslog szervert, ami összegyűjti SSL/TLS hitelesítés segítségével a logokat a hálózatbó, és továbbítja a LibreNMS-nek, viszont ez sajnos nem teszi bele a saját logjai közé, így külön fileokban tárolódnak a KKK-LIN szerveren.

**A szolgáltatás telepítése (CÍM)**

A syslog szolgáltatáshoz, pontosabban az Rsyslog-hoz a következő csomagokra van szükség:

* rsyslog
* rsyslog-gnutls
* gnutls-bin

A szolgáltatáshoz azért van szküség erre a három csomagra, hogy az SSL/TLS hitelesítéshez szükséges modulokat is telepítse.

**A szolgáltatás konfigurálása (CÍM)**

A Rsyslognak alapvetően van egy fő konfigurációs fájlja a */etc/rsyslog.conf*, ami behúzza az összes *.conf*-ra végződő fájlt a */etc/rsyslog.d/* útvonal alól. Emiatt és a könyebb átláthatóság miatt ebbe a mappába készítettük el a konfigurációs fájlokat. Két fájlt készítettünk, az első a *server.conf* nevű fájl:

# Listen on TCP 6514 with TLS

global(

DefaultNetstreamDriver="gtls"

DefaultNetstreamDriverCAFile="/cert/ca.crt"

DefaultNetstreamDriverCertFile="/cert/mail.crt"

DefaultNetstreamDriverKeyFile="/cert/mail.key"

)

module(

load="imtcp"

StreamDriver.Name="gtls"

StreamDriver.Mode="1"

StreamDriver.AuthMode="anon"

)

input(

type="imtcp"

port="6514"

address="0.0.0.0"

)

input(

type="imtcp"

port="6514"

address="::"

)

$template remote-incoming-logs, "/var/log/remote/%HOSTNAME%.log"

\*.\* ?remote-incoming-logs

A konfigurációs fájl több részből tevődik össze, amit az *x. táblázatban* olvashatnak.

|  |  |
| --- | --- |
| global direktíva | Megadjuk a titoksítás értékeit, illetve a tanusítványokat |
| modul direktíva | Betölti az *imtcp* modult, ami a logok fogadásáért van, ezen kívül beállítja a gnutls segítségével az SSL/TLS fogadás módját |
| input direktíva (IPv4) | Az összes IPv4-es interfacen a TCP 6514-es porton hallgat |
| input direktíva (IPv6) | Az összes IPv6-os interfacen a TCP 6514-es porton hallgat |
| template | Megadja, hogy ennek minden beérkező logot, a kliens hosztnevének megfelelő fájlba helyezzen, így szeparálva a jobb átláthtóság érdekében |

*x. táblázat - /etc/rsyslog.d/server.conf leírása*

Ezen kívül van még egy fájl, ami arra szolgálna, hogy a LibreNMS-nek az 514-es UDP porton keresztül továbbítsa a logokat fájlok alapján. Ez a fájl a *send.conf*:

module(load="imfile")

# KKK-LIN

input(

type="imfile"

File="/var/log/remote/KKK-LIN.log"

Tag="KKK-LIN"

Severity="info"

Facility="local6"

)

# KKK-VPN

input(

type="imfile"

File="/var/log/remote/KKK-VPN.log"

Tag="KKK-VPN"

Severity="info"

Facility="local6"

)

\*.\* @127.0.0.1:514

A részeinek leírását a(z) *x. táblázatban* láthatják.

|  |  |
| --- | --- |
| modul direktíva | Betöltjük a imfile modult (egy fájl továbbítása) |
| input direktívák | A fájl változást néző direktívák külön logfájlokra |
| log továbbítás | Az input direktívában meghatározott log fájlok továbbítása a szerver 514-es UDP portjára |

*x. táblázat - /etc/rsyslog.d/server.conf leírása*

**A szolgáltatás tesztelése (CÍM)**

A tesztelés során újraindítottunk az apache szervert a KKK-LIN szerveren, valamint kilistáztuk a */var/log/remote/* mappa tartalmát, ami megmutatja, hogy több log fájl található már itt, aminek van tartalma (későbbiekben lesz még róla szó). Ezeket a *x-y. képeken* láthatják.

|  |
| --- |
| *x. kép - /var/log/remote/ mappa tartalma* |
| *x. kép - /var/log/remote/KKK-LIN.log apache2 újraindítás* |

KKK-VPN

Szerver telepítése és beállításai

A Linux szervereinken a Debian 12.7-es verzióját használjuk, és grafikus felület nélküli telepítést végzünk, mivel a konfigurációs feladatokhoz nincs szükség GUI-ra és így jobb lesz a szerver erőforráskihasználása. A telepítés során megadott értékeket az *x-y. képeken* láthatják.

|  |
| --- |
| *x. kép - Hosztnév* |
| *A képen szöveg, képernyőkép, sor, Betűtípus látható  Automatikusan generált leírás x. kép – Domain név* |
| *x. kép – A szervere telepítése alatt feltelepített csomagok* |

A következő (*x. kép*) képen a szerver IP beállításai tekinthetők meg:

|  |
| --- |
| *x. kép – IP beállítások (majd meg ide meg kell csinalni)* |

A szerverre pár egyéb csomagot is telepítettünk, ami még a szerver alapvető kezeléséhez szükséges. Ezek a(z):

* mc (GUI-s fájlkezelő)
* dnsutils (DNS lekérdezésekhez szükséges parancsok)
* net-tools (IP cím, interfész konfigurációs beállítások)

Wireguard

A Wireguard szolgáltatásra azért volt szükség, hogy távolról is elérhető legyen az email szolgáltatás és a Pythonos weboldal. A Wireguard egy olyan VPN kliens, ami biztonságos, és megfelelő titkosítást nyújt az adatok védelme érdekében. A KKK-VPN szerveren egy ASA mögött található azért, hogy minél jobban meg legyen szűrve az a forgalom, ami nem engedélyezett.

**A szolgáltatás telepítése (CÍM)**

A VPN szolgáltatás telepítéséhez, a *wireguard* csomagot telepítettük le. Ez minden parancsot elérhetővé tesz nekünk, ami a konfigurációhoz szükség van. Ezen kívül az *ldap-utils* szolgáltatást a később olvasható scripthez.

Ahhoz, hogy a becsatlakozó kliensek elérjék a szolgáltatásokat a hálózatból, az *frr* nevű csomagot is telepítettük, ami OSPF forgalomirányító protokollt segítségével beroutolja a hálózatba a forgalmat.

**A szolgáltatás konfigurálása (CÍM)**

Mivel alapból nem érkezik konfigurációs fájlal a wireguard, ezért sajátot kell létrehozni. Viszont mivel a létrehozás során minden felhasználónak külön kulcsot hozunk létre, ezért egy shell scripetet írtunk a konfigurációs fileok létrehozására, amit a következőekben láthatnak:

#!/bin/bash

# LDAP server details

LDAP\_SERVER="ldap://kkk-adds.kkk.com"

BASE\_DN="ou=Felhasznalok,dc=kkk,dc=com"

BIND\_DN="cn=Administrator,cn=Users,dc=kkk,dc=com"

BIND\_PASSWORD="Password123"

i=3

echo -e "[Interface]\nPrivateKey = uGA+0Q9KV8cTEm+4eew0seQ8F8y0PNdcvAC8X4tpPXc=\nAddress = 10.99.99.2/24, 2001:db8:c1c1:9999::2/64\nListenPort = 51820\n" > /etc/wireguard/wg0.conf

# Perform LDAP search and extract sAMAccountName

sAMAccountNames=$(ldapsearch -x -H "$LDAP\_SERVER" -b "$BASE\_DN" -D "$BIND\_DN" -w "$BIND\_PASSWORD" "objectClass=person" sAMAccountName | grep "^sAMAccountName: " | sed 's/^sAMAccountName: //')

sr\_publickey=$(cat /etc/wireguard/public.key)

# Loop through each sAMAccountName

for accountName in $sAMAccountNames; do

echo "Processing user: $accountName"

mkdir -p "/etc/wireguard/cert/$accountName"

cd "/etc/wireguard/cert/$accountName"

wg genkey | tee "./private-$accountName.key"

chmod go= "./private-$accountName.key"

cat "./private-$accountName.key" | wg pubkey | tee "./public-$accountName.key"

privatekey=$(cat "./private-$accountName.key")

cl\_publickey=$(cat "./public-$accountName.key")

echo -e "[Interface]\nPrivateKey = $privatekey\nAddress = 10.99.99.$i/24, 2001:db8:c1c1:9999::$i/64\nDNS = 10.11.113.10, 2001:db8:c1c1:abfa::10/64\n\n[Peer]\nPublicKey = $sr\_publickey\nEndpoint = 10.11.113.2:51820\nAllowedIPs = 0.0.0.0/0, ::/0" > "./wg-$accountName.conf"

echo -e "\n# $accountName\n[Peer]\nPublicKey = $cl\_publickey\nAllowedIPs = 10.99.99.$i/32, 2001:db8:c1c1:9999::$i/128" >> /etc/wireguard/wg0.conf

i=$((i + 1))

done

Ez a fájl elkészíti a szerver konfigurációs fájlját pont mint az össze felhasználónak az összes felhasználónak, akik az Active Directory Domainen belül vannak. Ez a script csak a fő épületben lévő felhasználóknak készíti el ezeket, van 2 további shell scriptünk, ami a másik két sitenak ugyanezt megcsinálja csak a keresési zóna az adott fő OU.

Ezzel elkészül a konfiguráció, a fájlokat minden felhasználónak a saját meghajtójára másoljuk, valamint emailen keresztül kiküldjük nekik, amitől kezdve ők kezelhetik a saját fájlukat, ha elveszik újra oda lehet adni nekik, illetve lehet újat is generálni, viszont, ekkor minden felhasználónak újra ki kell küldeni az új konfigurációs fileokat.

Az *frr* konfigurálásához a */etc/frr/daemons* fájlban a következő változtatásokat végeztük el:

…

ospfd=yes

ospf6d=yes

…

Ezzel engedélyeztük a szolgáltatást. A konfiguráció további lépései úgy működtek, mint egy cisco eszközön. A *vtysh* parancs kiadása után (bashben), egy új shell nyílt meg ami, mint említettük, egy Cisco eszköz konfigurációját szimulálja. A konfiguráció mentésével az */etc/frr/frr.conf* fájl írja a szolgáltatás majd egy újraindítást követően a szerver már működőképes. A konfigurációs fájl így néz ki:

ide majd be kell illeszteni, élesben

A következő képen pedig a routing tábláját láthatjuk *vtysh* shellen keresztül a KKK-VPN szervernek.

**A szolgáltatás tesztelése (CÍM)**

A szolgáltatást Kovács Gábor IT-s szakember bejelentkezésével teszteltük. Kliensoldali csatlakozás és logok alapján, valamint az IP beállítások és pingelés alapján mutatjuk be, hogy a VPN kapcsolat sikeres. Ezeket a *x-y. képeken* láthatják.

|  |
| --- |
| *x. kép – Aktív kapcsolat* |
| *x. kép – Kliens logjai a kapcsolatról* |
| *x. kép – IP beállítások a kliensen* |
| *x. kép – Wireguard interface a szerveren* |

Rsyslog kliens

A logokat a KKK-LIN szerveren gyüjtjük, ezért rsyslog segítségével, SSL/TLS titkosítással továbbítjuk a szerver összes logját a log szerverünk felé.

**A szolgáltatás telepítése (CÍM)**

A megfelelő működéshez három csomagra telepítésére volt szükségünk, ezek a(z):

* rsyslog
* rsyslog-gnutls
* gnutls-bin

Ezek a csomagok biztosítják magának a syslog meglétét, illetve azt, hogy a szerver biztonságosan továbbíthassa a logokat.

**A szolgáltatás konfigurálása (CÍM)**

A szolgáltatás kliensoldali konfigurációja során, átmásoltam a szükséges tanúsítványokat a szerverről, amik segítségével titkosítja a szerver a logokat a küldés során. Ezt követően a */etc/rsyslog.d/* mappába létrehoztam egy *send.conf* nevű fájlt, mivel az */etc/rsyslog.conf* fájl behúzza az összes fájlt abból a mappából ami .conf-ra végződik, ezért a konfigurációhoz inkább készítettünk egy külön fájl, aminek segítségével jobban átlátható a konfiguráció.

A következő kódrészlet szolgálja az összes log továbbítását a KKK-LIN szerverre:

$DefaultNetstreamDriverCAFile /cert/syslog/ca.crt

$DefaultNetstreamDriverCertFile /cert/syslog/client.crt

$DefaultNetstreamDriverKeyFile /cert/syslog/client.key

$DefaultNetstreamDriver gtls

$ActionSendStreamDriverMode 1

$ActionSendStreamDriverAuthMode anon

\*.\* @@kkk-lin.kkk.com:6514

**A szolgáltatás tesztelése (CÍM)**

A szolgáltatás teszteléséhez újraindítottuk az *frr* szolgáltatást, aminek a logjait a KKK-LIN szerverről mutatjuk be. Ezeket az *x-y. képeken* láthatják.

|  |
| --- |
| *x. kép – frr szolgáltatás újraindítása* |
| *x. kép - /var/log/remote/KKK-VPN.log fájl utolsó sorainak megjelenítése* |