
redhat Wallpaper by M. Erhardt

RHEL 7 Arabic Notes

تلخيص الطالب : أحمد عبدالمنعم

فيديوهات المهندس : مصطفى حموده

رابط ال Play List

https://www.youtube.com/playlist?list=PLy1Fx2HfcmWBpD_PI4AQpjeDK5-5q6TG7

شوية ملاحظات

1- هذه الملخصات هى عبارة عن مجرد تجميع للمعلومات وتمت ازالة كل الكلام الذى ليس له علاقة بالكورس ، من الاخر كده اللى هنا بس هو المختصر المفيد والكلام مكتوب باللهجة المصرية مع مراعاة التوضيح لاقصى درجة

2- التلخيص ده خاص بفيديوهات البشمهندس مصطفى حموده بس ، يعنى حضرتك هتتفرج على الفديوهات وتقرأ من التلخيص

3- كمان هتلاقى ملاحظات انا جبتها من النت علشان تساعدك انك تفهم اكتر وبالمناسبة كمان انا حطيت لينكات لمواضيع كتيرة متعلقة بالتراك ده ممكن انت تقرأها على النت هتفيدك جدا

4- ملحوظة اخيرة وهى ان التراك ده بدايته من الفديو رقم 66 اليوم ال 35 وده عنوان الفديو

66-Day-35 DHCP_Server

لحد الفديو رقم 85 اليوم ال 49 وده عنوان الفديو

85-Day-49 BIND Cont-4

تنبيه بسيط وهو ان التراك التالت ده لسه ناقص فيه مواضيع كتيرة زى ال

1-Samba

2-GPG

3-SSH

4-Firewall

5-PXE Boot

6-SeLinux

7-NTP

8-SNMP

9-Mail Server

طيب انت لو عايز تذاكر المواضيع دى ، هتضطر انك تراجعها من المنهج القديم الخاص ب **RHEL 6** وده لينك ال **Playlist** اللى فيها باقى المواضيع القديمة

https://www.youtube.com/playlist?list=PLCIJjtzQPZJ_10_h-jzD299qkg_IuoT-5

وده لينك موقع **Certdepot** هتلاقى عليه اغلب المواضيع اللى ممكن تحتاجها

https://www.certdepot.net/

ملحوظة اخيرة خاصة بال **Play List** اللى مشروح فيها باقى مواضيع **Admin 3** اللى موجودة على قناة **FreeForArabs** ، عنوانين الفديوهات هناك مش واضحة بمعنى ان كل فديو هناك العنوان بتاعه مش بيوضح هو بيتكلم عن اى بالظبط ، فانا بما انى اتفرجت عليها هكتب لكم المواضيع اللى هناك بالترتيب من الفديو رقم 1 لحد الفديو رقم 28

اولا متنساش ده اللينك بتاعتها

https://www.youtube.com/playlist?list=PLCIJjtzQPZJ_10_h-jzD299qkg_IuoT-5

ودى بقى المواضيع بالترتيب

1-Network intro

2-Network basic

3-NTP + DHCP

4-NFS + FTP

5-FTP Cont + Special Permissions

6-DNS 1

7-DNS 2

8-DNS 3

9-DNS 4

10-Samba

11-GPG 1

12-GPG 2

13-SSH

14-Web Server

15-Virtual Host

16-Apache SSL + Xinetd + CUPS

17-Squid [Proxy Server]

18-New Starting Point

19-mysql + Firewall Introduction

20-Iptables-1

21-Iptables-2

22-Iptables-3

23-PXE Boot Intro

24-PXE& kickstart

25-Selinux

26-SNMP-1

27-SNMP-2

28-SNMP-3

التراك الثالث

Admin 3

Table Of Contents

1-DHCP

بداية التراك التالت

فى الغالب جزء ال **Authentication** وال **Policy** زى ال **IPA** وغيرها ، بيكون خاص بجزء ال Security ، مش مجرد انه جزء خاص بال Services وخلاص ، على الرغم من انه بيشتمل على انك هتشغل service ، **لكن فى فرق بين انك ت run service وبين انك ت configure secure service**

بداية من التراك ده لازم تتأكد ان ال **Package** بتاعت ال **service** اللى انت هتشتغل عليها ، لازم تكون متسطبة ولازم تكون **Up and running**

اول حاجة هنعملها وهى اننا هنسطب ال DHCP Service ، عن طريق الامر

yum install dhcp

تعالى بقى نشوف ال **status** بتاعت ال service دى

systemctl status dhcpd

ولو ملقتهاش active ولا enable ، يبقى تروح تعملها enable وكمان تخليها active

systemctl enable dhcpd

systemctl start dhcpd

ملحوظة وانت بتعمل start للـ dhcpd ممكن تطلعلك رسالة ال error دى

● dhcpd.service - DHCPv4 Server Daemon
Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; enabled; vendor preset: disabled)
Active: failed (Result: exit-code) since Tue 2018-07-03 05:46:20 EDT; 1min 13s ago
Docs: man:dhcpd(8)
man:dhcpd.conf(5)
Process: 2113 ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group dhcpd --no-pid (code=exited, status=1/FAILURE)
Main PID: 2113 (code=exited, status=1/FAILURE)

Jul 03 05:46:20 server.yum.com dhcpd[2113]: Internet Systems Consortium DHCP Server 4.2.5
Jul 03 05:46:20 server.yum.com dhcpd[2113]: Copyright 2004-2013 Internet Systems Consortium.
Jul 03 05:46:20 server.yum.com dhcpd[2113]: All rights reserved.
Jul 03 05:46:20 server.yum.com dhcpd[2113]: For info, please visit https://www.isc.org/software/dhcp/
Jul 03 05:46:20 server.yum.com dhcpd[2113]: Not searching LDAP since ldap-server, ldap-port and ldap-base...file
Jul 03 05:46:20 server.yum.com dhcpd[2113]: Wrote 0 leases to leases file.
Jul 03 05:46:20 server.yum.com systemd[1]: dhcpd.service: main process exited, code=exited, status=1/FAILURE
Jul 03 05:46:20 server.yum.com systemd[1]: Failed to start DHCPv4 Server Daemon.
Jul 03 05:46:20 server.yum.com systemd[1]: Unit dhcpd.service entered failed state.
Jul 03 05:46:20 server.yum.com systemd[1]: dhcpd.service failed.
Hint: Some lines were ellipsized, use -l to show in full.

فكك من الرسالة دى دلوقتى ، وتعالى بقى نتكلم عن ال DHCP

مبدئيا كده ال dhcp هو اختصار ل

Dynamic Host Configuration Protocol

يعنى اى بقى ؟ بص بكل بساطة كلمة configuration protocol معناها انه بروتوكول مسؤل عن انه يعمل autoconfiguration لل network بتاعت الاجهزة اللى موجودة ، وكلمة dynamic معناها انى مش لازم احط ال ip static بايدى على كل جهاز عندى لواحده

يبقى اذا ال DHCP هو عبارة عن بروتوكل كل وظيفته انه يديك setting خاصة بكل جهاز موجود عندك على الشبكة

طيب ال DHCP هيشتغل ازاى ؟؟ قالك خلى عندك سيرفر كده وخليه هو ال dhcp server وتعالى على جهاز ال client واعمله configure انه يستخدم ال dhcp protocol علشان يحاول ياخد ايبى من الشبكة اللى هى هنا ال dhcp server ، طيب الموضوع ده هيتم ازاى ؟؟ قالك ان عملية ال client ياخد ip من ال dhcp بتم على 4 خطوات اسمها **DORA** ودى اختصار ل

Discover Offer Request ACK

نمسكها كلمة كلمة ، اولا **discover** ، هنا انت عندك ان جهاز ال Client هيكون Configured انه يدور على ip من ال network ، فا هيعمل اي بقى ؟ هو هيبعت **BroadCast Packet** وال BroadCast Packet دى هتكون مبعوتة على Special Mac Address ، هو **FF:FF:FF:FF:FF:FF** ، اى الماك ادرس ده ؟ بكل بساطة انت لو ترجمته ل decimal هتلاقيه كده **255.255.255.255**

يبقى ال **Mac Address** ده عو عبارة عن ال broadcast ، وده بيبعته لاى جهاز فى الدنيا ، بمعنى ان انت لو عندك FTP Server ، برضو هيستقبل من جهاز ال Client ال Packet دى برضو وكذلك الامر برضو لو فيه اجهزة clients ، كلهم هيستقبلوا نفس ال Packet اللى جهاز ال client بعتها وبيطلب فيها انه عايز ياخد ip ، **كده المفروض مين اللى يرد عليه ؟؟**

المفروض اللى يرد عليه بس هو ال DHCP Server ؟ هيرد ويقوله خد ال ip ده وخد كمان ال netmask وخد كمان ال Gateway وممكن كمان يقوله خد ال DNS

يبقى جهاز ال Client بعت discover وجهاز ال dhcp server راح رد عليه ب offer ، طيب دلوقتى بقى لما ال DHCP Server يرد على جهاز ال Client اللى هو ممكن تسميه برضو dhcp client ، لما يرد عليه فى ال offer

هل هيرد عليه BroadCast تانية ؟؟ قالك لا طبعا ، لما ال DHCP Server يرد هيرد بحاجة اسمها **Unicast Packet**

طيب هيبعتها لمين بالظبط ؟ قالك هيبعتها لل Mac Address اللى بعت ال Request او اللى بعت discover

يبقى نفهم من اللى فات ان جهاز ال client بعت discover وراح ال dhcp server رد عليه ب offer يعنى بيعرض عليه هل يوافق على العرض اللى بعته وهو انه ياخد ال ip الفلانى ده وياخد ال netmask دى وياخد ال gateway دى ، يروح هنا بقى جهاز ال client يرد عليه ب request يعنى بطلب انه موافق على ال offer اللى عرضه ال dhcp وخلى بالك انه فى الخطوة التالتة دى جهاز ال client هيبعت برضو ال request على ال BroadCast

واخيرا تيجى الخطوة رقم 4 من ال dhcp server وهو بيرد على جهاز ال client بحاجة اسمها **ACK** اللى هى اختصار ل **Acknowledge** يعنى ال dhcp server بيأكد انه خلاص بعت ال ip وال gw الفلانى ده لل dhcp client اللى طلبهم

يبقى خليك فاكر ان ال Client بيبعت كل رسايله سواء discover او حتى request بيبعتهم ك **BroadCast** ، لكن ال Server بيرد ديما ب **unicast Packet**

ملحوظة مهمة وهى

[root@client ~]# route -n

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.1.1	0.0.0.0	UG	100	0	0	enp0s3
192.168.1.0	0.0.0.0	255.255.255.0	U	100	0	0	enp0s3

ال destination اللى هى **0.0.0.0** معناها انك لو عايز تطلع على مكان فى الدنيا ، يعنى لو عايز تروح لاى موقع مثلا ، يبقى انت هتطلع عن طريق ال Gateway دى **192.168.1.1**

طبعا لو عايز تعرف اذا كان الجهاز بتاعك واخد ip static ولا من ال dhcp ، عن طريق الامر

nmcli connection show enp0s3

وممكن تجيب تفاصيل Profile معينة عارف عن طريق الامر

ifconfig enp0s3

طيب افرض بقى ان ال Network Manager مش موجود اصلا ، ممكن تروح تشوف الملف ده

less /etc/sysconfig/netwotk-scripts/ifcfg-enp0s3

TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="dhcp"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="enp0s3"
UUID="59afa824-d966-424a-bb92-83ae974c6e5d"
DEVICE="enp0s3"
ONBOOT="yes"

ملحوظة مش معنى ان الملف ده فى

BOOTPROTO="dhcp"

يبقى انت كده واخد من ال dhcp ، وبالمناسبة كمان انت ممكن تغير ال ip عن طريق ال ifconfig

ifconfig enp0s3 192.168.1.7/24

كده انت عندك 4 طريق علشان تغير ال ip

بص بقى لو انت عندك جهاز ومش شغال بال network manager وعايز تعرف اذا كان واخد ip من ال dhcp ولا لأ ، هتلاقى ملف كده اسمه

less /var/lib/dhclient/dhcp.lease

طب انت هتقول ان RHEL 7 اصلا شغالة بال Networkmanager ب by Default يبقى برضو هتلاقى فى المسار ده

less /var/lib/NetworkManager/dhclient-59afa824-d966-424a-bb92-83ae974c6e5d-enp0s3.lease

ملف امتداده

.lease

واللى جمبه ده هو ال **UUID** بتاع ال **enp0s3 Profile**

والملف ده بيكون فيه كذا **lease** ، يعنى كذا section وكل lease فيهم فيه كل المعلومات اللى انت خدتها

الملف ده بقى فيه كل المعلومات اللى ال Network Manager طلبها من ال DHCP لما قام ، ويبقى كده طلعنا بقاعدة وهى انك طالما لقيت ملف ال **lease.** ده يبقى تعرف ان ال Interface ده معمول ليه configured او هو اوتوماتيك بياخد ip من ال dhcp

تعالى بقى نفتح الملف ده ، اول حاجة عندك السطر ده

option dhcp-lease-time 86400;

خلى بالك بقى ان ال client مش هياخد ال ip مدى الحياة ، ده هياخده لمدة محددة ، يبقى هنا ال lease time ، يعنى المدة اللى ال ip اللى انت خدته هيبقى معاك فيها هتكون 86400 ثانية يعنى 1440 دقيقة يعنى 24 ساعة وبيقولك كمان انك لازم تعمل اعادة تجديد فى الوقت المحدد

renew 2 2018/07/03 20:21:40;

وبالمناسبة انت لازم تبص على التاريخ بتاع كل **lease** ، ليه ؟ لان انت ممكن تكون اخر lease انت خدته من اسبوع مثلا وبالتالى انت كده هتلاقى الملف موجود

يبقى انت لازم تشوف الوقت بتاعتك كام بالظبط؟؟ وتشوف ال 3 اسطر دول

renew 2 2018/07/03 22:52:29;
rebind 3 2018/07/04 08:10:20;
expire 3 2018/07/04 11:10:20;

يعنى تشوف انت لازم تجدد ال ip امتى بالظبط ، ولو لقيت الوقت منتهى اصلا ، يبقى تعرف انك كده واخد من ال dhcp

يبقى هنا اى اللى هيحصل لو انت سبت الجهاز لحد ما ال

expire 3 2018/07/04 11:10:20

ياجى ؟ هيحصل حاجتين ، يا اما انك هتعمل renew من ال dhcp ، او يا اما انك مش هتلاقى ال dhcp وبالتالى مش هتعرف تعمل renew وبالتالى انت مش هتستخدم ال ip اللى انت خدته المرة اللى فاتت
يعنى اصلا ال DHCP Server هيديك ip وهيحددلك وقت لل expiration بتاعته

كده انا عندى مشكلتين ، المشكلة الاولى وهى افرض ان جهاز ال client وهو بيعمل renew لل ip راح لقى ال dhcp server كان بيعمل restart مثلا او مش موجود ، اى بقى اللى هيحصل وقتها؟

ببساطة الاجابة موجودة فى ال 3 سطور دول

renew 2 2018/07/03 22:52:29;
rebind 3 2018/07/04 08:10:20;
expire 3 2018/07/04 11:10:20;

اصلا ال dhcp بيقول لل client انت المفروض تسألنى على ip جديد ، وهل هتكمل مع ال ip اللى انت خدته ده ولا لأ ، مش كده وبس ، ده كمان هيديله حاجة اسمها expire

طيب افرض ان انت جيت تعمل renew وملقتش السيرفر ؟ المفروض اصلا وانت بتعمل configure لل dhcp server تديله حاجة اسمها ال **grace period** اللى هى فترة السماح ، بمعنى ان جهاز ال DHCP Server وهو بيدى ال ip لجهاز ال Client هيقوله لو انت مقدرتش تعمل communicate معايا وتاخد ip جديد فانت عندك فترة سماح هديهالك قد تكون مثلا 4 ساعات او 6 ساعات تحاول خلال الفترة دى انك تخلى معاك ال ip اللى انا عطتهولك ، طبعا خلال الفترة دى هو هيكون بيحاول انه يتصل بال dhcp server علشان يجدد ال ip بتاعته ، طيب افرض انك برضو معرفتش تعمل communicate مع ال dhcp server خلال الفترة دى ، يبقى كده خلاص ال ip بتاعتك هيحصله expiration

يبقى الشرح من تانى ، اولا السطر ده

renew 2 2018/07/03 22:52:29;

معناها ان فى الوقت ده هيبدأ يعمل renew ، طيب وبعدين

ندخل على السطر ده

rebind 3 2018/07/04 08:10:20;

كده الفترة بين السطرين دول ، يعنى حوالى من الساعة 10 بالليل لحد الساعة 8 الصبح دى فترة السماح اللى انت هتحاول تتصل بيها بال dhcp server علشان تأكد على ال ip بتاعك ، او علشان تاخد منه ip جديد ، طيب افرض ملقتوش ، **يبقى نخش على السطر التالت**

expire 3 2018/07/04 11:10:20;

كده الفترة بين السطر التانى والتالت اللى هى ساعتين ، اللى هما خلال الوقت ده بس ممكن تستخدم ال ip القديم اللى انت خدته من ال DHCP Server وبعدها هينتهى وبالمناسبة ال value بتاعت الوقت دى Configured

طيب عندنا بقى سؤال هنا ، وهو لو انت system admin وشغال فى شركة كبيرة وليكن عندك مثلا 500 جهاز موصلهم على DHCP Server ، وفرضا بقى ان مواعيد شغلك من 8 الصبح ل 6 المغرب

يبقى المفروض تعمل configure ل value زى دى تخليها اى بالظبط ؟؟

السؤال بشكل اصعب ، هل المفروض ال values بتاعت ال dhcp تكون كبيرة ولا صغيرة ولا اى بالظبط ؟ يعنى لما ادى ip لل Client اديله ip لمده اسبوع ولا شهر ولا اى بالظبط ؟

بص انت عندك مشكلة لو انت مثلا عطيت لكل جهاز عندك static ip لمدة اسبوع مثلا ، لان على افتراض ان انت عندك ال users بيروحوا وياجاوا يعنى اجهزتهم مش ثابته فى مكانها فى الشركة وبكده ال ip address اللى عندك هتخلص ، وانت اصلا لما بتيجى تعمل configure لل DHCP بتقوله ان لما حد ياخد منك ip يبقى ياخد من ال subnet المعينة دى ، يعنى مثلا بتكون /24 يعنى بتدى عدد 255 **ايبى** ، شيل منهم ال gateway ip يبقى انت عندك 253 ايبى ك Maximum عدد من الايبهات

طيب برضو لو انت خليت ال value بتاعت ال **renew ip** قليلة جدا مثلا ساعتين ، يبقى انت عندك ال BroadCast هيزيد جدا ، يبقى لو انت مثلا عندك 200 جهاز وال 200 جهاز دول بيعموا كل ساعتين BroadCast يبقى انت كده هيكون عندك ما يسمى بال **BroadCast Storm** شبه ال DDOS Attack ، معنى كده ان انت لازم تحط values محترمة وال value دى تكون على حسب عدد الاجهزة اللى عندك وشغلهم هيكون ازاى برضو

والسيناريو المفضل نوعا ما ، انك لو الاجهزة اللى عندك متصلة عن طريق ال **wired** ، يبقى ال renew value تكون مش اقل من **8 ساعات** وتخلى ال expire time بتاعته **16 ساعة** او خليه مثلا 12 ساعة ، طيب لو الاجهزة بقى متصلة عن طريق ال **wireless** ، يبقى تحاول تخلى ال lease time اللى هى فترة السماح بتاعت الاجهزة كل ساعتين ، والسبب ان طبيعة ال wireless مختلفة تماما عن طبيعة ال wired خالص ، طبيعتها ان كل شوية واحد عمال يتصل وواحد يفصل ، واحد يفصل وواحد يتصل وهكذا وخلى ال renew time بتاع الاجهزة يكون كل 2.5 او 3 ساعات

تعالى بقى نرجع نحل المشكلة بتاعت ال dhcp

● dhcpd.service - DHCPv4 Server Daemon
Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; enabled; vendor preset: disabled)
Active: failed (Result: exit-code) since Tue 2018-07-03 05:46:20 EDT; 1min 13s ago
Docs: man:dhcpd(8)
man:dhcpd.conf(5)
Process: 2113 ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group dhcpd --no-pid (code=exited, status=1/FAILURE)
Main PID: 2113 (code=exited, status=1/FAILURE)

اولا ملف ال configuration بتاع ال dhcp موجود فى المسار

cd /etc/dhcp/dhcp.conf

وتفاجىء انه ملف ال configuration فاضى اصلا ، يعنى مفيش اصلا ملف configuration ، فاكر بقى ايام ال man pages ؟

فانت خلى بالك بقى من المسار ده اللى فيه كل ملفات ال docs بتاعت معظم ال services اللى موجودة

cd /usr/share/doc/

انت هنا لما سطبت ال dhcp راح عمل example file فى المسار ده

/usr/share/doc/dhcp/dhcp-4.2.5/dhcpd.conf.example

طيب تعالى كده ناخد نسخة من الملف ده ونوديها لمكان ا ل configuration بتاعت ال dhcp ، نفذ الامر ده

cp /usr/share/doc/dhcp/dhcp-4.2.5/dhcpd.conf.example /etc/dhcp/dhcpd.conf

ملحوظة : متنساش حرف ال d وانت بتكتب اسم ال service اختصارا ل Daemon

تعالى بقى نفتح الملف ده ونغير فيه ال settings بتاعته

واول حاجة انا عملتها انى غيرت ال domain name

option domain-name "ahmed.org";

وبعدين هغير ال domain name server ، ممكن اروح اجيب من جوجل ال Open DNS Server

option domain-name-servers 208.67.222.222, 208.67.220.220;

وبعد كده ممكن اغير ال **default lease time** ، مثلا اخليه

default-lease-time 3600;

يعنى كل ساعة ، يعنى كده ال default lease time معناه انى لما ادى ip للل Client يبقى ال Client لازم يرجع يعمل renew منى كل 3600 ثانية يعنى كل ساعة اما بقى بالنسبة لل

max-lease-time 7200;

فده معناه ان بعد ساعتين لو جهاز ال client ملاقنيش ، يبقى خلى ال ip ده معاه مثلا 7200 ثانية يعنى 120 دقيقة

وفى كمان option عندك فى الملف ده برضو معمول عليه comment وهو

#authoritative

يعنى لو لغيت ال comment فانت كده بتقوله ان ده هو ال Official DHCP بتاعك ، وده هيفيدك جدا فى حالة ان انت عندك اتنين dhcp servers ، وبالمناسبة ده مش شىء طبيعى لما يكون شبكة واحدة وفيها اتنين dhcp servers وكمان الاتنين مش شغالين مع بعض

كده انت بتعذب نفسك ؟ ليه بقى لان انت عندك مثلا ممكن ال DHCP الاولانى يدى ip وال DHCP التانى يدى نفس ال ip وفى الحالة دى هيحصل ip conflict وهيبقى عندك مشكلة فى الشبكة ، يبقى انت تخلى واحد فيهم هو ال **authoritative** ويستحب انك تعملها يعنى يكون هو الرسمى

بعد كده بقى ممكن تيجى من اول السطر ده

 # DHCP server to understand the network topology.

وتمسح بقية الملف للاخر ن يعنى هستخدم ال **vim** ، واول حاجة تعمل set number يعنى ترقم الملف بتاعتك، يبقى تروح لل execution mode وبعدين تنفذ

:.$d

كده هيمسح من اول ما ال cursor واقف لحد الاخر

طيب فى ملحوظة مهمة بخصوص ملف ال configuration بتاع ال DHCP ، بيقولك بقى ان اى حاجة هتعرفها فوق فى ملف ال Configuration ده وتكون Globally ، فالحاجة دى هتطبق على اى subnet انت هتعملها تحت فى الملف ، لكن اللى هيتعرف جوه ال subnet يعنى هيكون جوه القوسين بتوع ال subnet هيكون خاص بال subnet دى بس

```
subnet 10.5.5.0 netmask 255.255.255.224 {
   range 10.5.5.26 10.5.5.30;
   option domain-name-servers
ns1.internal.example.org;
   option domain-name "internal.example.org";
   option routers 10.5.5.1;
   option broadcast-address 10.5.5.31;
   default-lease-time 600;
   max-lease-time 7200;

}
```

يعنى مثلا لو عرفت NTP Server جوه ال subnet دى هيفضل ال ntp موجود بشكل Locally لل Subnet دى ، يعنى مثلا لو عندك ال domain name ده

```
option domain-name "internal.example.org";
```

فده هي reflect ال Subnet دى بس

تعالى بقى نعدل فى ال subnet دى ، اول حاجة هغير ال ip واخليه مثلا

192.168.21.0

بعد كده ال rang اللى هيحكمنى ، يعنى هيبدأ يوزع ايبهات من اول كام

ممكن اخليه كده

range 192.168.1.5 192.168.1.250

طيب سؤال احنا ليه بدأنا نوزع ايبهات بداية من 192.168.121.5 وانتهينا عند 192.168.21.250 ، لان خلى بالك ان الجماعة بتوع ال Network Administrator ديما بيحجزوا ال Gateway يا اما انه يكون فى بداية ال subnet او يكون فى نهايته عادى متستغربش ان ا ل GW ممكن يكون فى اخر ال subnet ، يبقى انت تخليك ذكى شويتين وتبدأ توزع ايبهاتك بعد ما تسيب اول 3 او 4 ايبهات فى اول واخر ال subnet

بالنسبة بقى للسطرين دول

option domain-name-servers ns1.internal.example.org;

option domain-name "internal.example.org";

اللى هما ال Domain Name وال Domain Name Server ، فانت اصلا مش محتاجهم يعنى ممكن تمسحهم ، لان انت عرفتهم Globally فوق فى بداية الملف

وبعدها بقى ال

option routers

وبعدها ال BroadCast Address اللى هو نهاية عدد الايبهات فى الشبكة بعد كده هتقولى فين ال DNS ، هقولك ما انا عرفته فوق اصلا Globally

تعالى بقى نعمل reboot لجهاز ال client

وبعدها ممكن تنفذ الامر ده علشان تشوف جهاز ال client وهو بياخد ip من ال dhcp server

tail -f /var/log/messages

هتلاقى هنا الجهاز بتاعك وهو بيدى ip لجهاز ال client

Jul 3 11:29:00 server dhcpd: DHCPDISCOVER from 08:00:27:22:7f:98 via enp0s3
Jul 3 11:29:00 server dhcpd: DHCPOFFER on 192.168.1.9 to 08:00:27:22:7f:98 (client) via enp0s3
Jul 3 11:29:00 server dhcpd: DHCPREQUEST for 192.168.1.9 (192.168.1.3) from 08:00:27:22:7f:98 (client) via enp0s3
Jul 3 11:29:00 server dhcpd: DHCPACK on 192.168.1.9 to 08:00:27:22:7f:98 (client) via enp0s3

فى الاربع سطور دول هتلاقى ال **DORA** ، بداية من ال **Discover** ثم ال **Offer** ثم ال **Request** ثم ال **ACK**

تعالى بقى على جهاز ال client علشان تتأكد ان ال lease جى من انهى dhcp server بالظبط ؟

less /var/lib/NetworkManager/dhclient-59afa824-d966-424a-bb92-83ae974c6e5d-enp0s3.lease

بص بقى على اخر lease فى الملف ده

```
lease {
  interface "enp0s3";
  fixed-address 192.168.1.9;
  option subnet-mask 255.255.255.0;
  option routers 192.168.1.1;
  option dhcp-lease-time 600;
  option dhcp-message-type 5;
  option domain-name-servers
208.67.222.222,208.67.220.220;
  option dhcp-server-identifier 192.168.1.3;
  option broadcast-address 192.168.1.55;
```

```
  option domain-name "ahmed.com";
  renew 2 2018/07/03 15:37:46;
  rebind 2 2018/07/03 15:42:18;
  expire 2 2018/07/03 15:43:33;
}
```

بص كده على ال

```
  option domain-name "ahmed.com";
```

شوف كده هو بياخد منين بالظبط وبالنسبة للملف بتاع ال

less /var/lib/NetworkManager/dhclient-59afa824-d966-424a-bb92-83ae974c6e5d-enp0s3.lease

هتلاقى برضو اسم الجهاز اللى طلب منك ال ip ، عندى انا مثلا مسميه client

Jul 3 11:33:33 server dhcpd: DHCPREQUEST for 192.168.1.9 from 08:00:27:22:7f:98 (client) via enp0s3

وديما اتأكد انك لما تعمل configure لل DHCP اتأكد ان انت معندكش

dhcp 2 ، الحاجة التانية وهى اختار lease time يكون مناسب للشبكة بتاعتك

حاجة اخيرة فى ال DHCP وهو انه بيشتغل على UDP Connection وبيشتغل كمان على بورت 67

2-iSCSI Server

بدأنا فى ال iSCSI ، بداية كده تخيل ان انت عندك سيرفر معين ، تفتكر اكبر عدد من الهاردات ممكن تضيفها للسيرفر ده اي ؟ هتقولى على حسب ال slots اللى موجودة فى ال MB

حلو خالص فانت فى البداية كده عندك مشكلة وهى ان عدد الديسكات اللى هتركب فى السيرفر ده هتكون Limited جدا ، العدد نفسه limited ، ومش كده وبس لازم تسأل ال Performance بتاع الديسكات دى هيكون اى بالظبط ، طب افرض بقى ان انت عايز سيرفر واحد يكون عليه بتاع 50 تيرابابت او 100 تيرابايت مثلا هتعمل اى ؟

فالناس فكرت وقالت طب ما انا اصلا عندى ال Storage Solutions الكبيرة موجودة اصلا ، ودى عبارة عن انك بتجيب راك كبير كده وبيكون مليان Slots وراكب فيه ديسكات كتيرة

مش كده وبس دا احنا ممكن نضرب الديسكات الكتيرة دى كلها مع بعض فى الخلاط ونطلع Storage Pool كبيرة ونبدأ اننا نشير لكل Server لوحده ال Storage الكبيرة دى

ودى اسمها بقى **Shared Storage** ، يعنى بكل بساطة بيكون عندك Storage كبيرة فشخ وبيكون في اكتر من سيرفر بي Access ال Storage

والناس فكرت فى الحوار ده لعدة اسباب ، منها وهى ان ال Storage بتكون موجودة كلها فى مكان واحد بس بتتأكسس من كذا سيرفر ، الحاجة التانية وهى انى خلاص مش لازم اشترى high in server يعنى ممكن اجيب Low in Servers يعنى سيرفرات صغيرة جدا فيها مثلا 4 slots بس مش هحط عليها غير 2 ديسكين بس وفى نفس الوقت هخليها تشوف ال Storage من ال Shared Storage اللى انا عملتها

وطبعا ال Shared Storage سعرها عالى ومفيش مشاكل على كده بس طبعا هزود ال Performance بتاعها بشكل كبير جدا وطبعا هزود الحجم بتاعها بشكل كبير جدا وبكده بدل ما يكون عندى سيرفر واحد او 500 سيرفر وكل واحد فيهم ليه ال Storage الخاصة بيه ، لا انا هخليهم كلهم ي Access ال Shared Storage دى

وده هيفدك فى سيناريوهات كتيرة جدا وعندك اشهر سيناريو موجود وهو ان انت يكون عندك Virtual Machines تكون running ، ولو عندك Virtual Machines وعايز تعمل Enable ل Feature معينة زى ال High Availability ففى الحالة دى يبقى لازم كل السيرفرات تعمل Access لنفس ال Shared Storage فى نفس اللحظة

وبالتالى لو ال Storage بتاعتك Local بس على قد السيرفر يبقى انت كده عمرك ما هيكون عندك High Availability بالنسبة لل VMs دى مثلا وده طبعا فى حد ذاته مشكلة

انت بقى علشان تعمل حاجة زى دى ، بيقولك ان فى Implementations كتيرة اتعملت ، او اتعملت مجموعة Protocols اشهرها هو ال

FC ====> Fiber Channel

وال

FCOE =====> Fiber Channel Over Ethernet

وال

iSCSI ===> Internet Small Computer System Interface

طيب من سنين كتيرة كده لحد 2008 وكان ال FC هو اللى مسيطر على السوق وفى حوالى 2011 بدأ يظهر ال FCOE وبداية من 2013 بدأ ال iSCSI يظهر تانى فى السوق

وبالمناسبة ال iSCSI كان موجود طول الفترة اللى فاتت دى بس طبعا مكنش ليه شهرة كبيرة فى عالم الداتا سنتر لمجموعة اسباب كده ممكن نتكلم عنها

يعنى مثلا ال Fiber Channel وقتها كان عبارة عن كروت نت بتجيلك وكانت الكروت دى بتديك 2G او 4G ولما وصل 8G كان اختراع كبير فى الوقت ده ، طبعا حاليا ال FC ممكن يوصل معاك ل 16 جيجا ، بمعنى ان اللينك اللى واصل بين السيرفر وبين ال switch اللى واصل فى النصف علشان يروح لل Storage كان سرعته بتبقى 16 جيجا وده طبعا كان اختراع

اما بقى بالنسبة لل Fiber Channel Over Ethernet ، فده كان عبارة عن Cable عادى جدا بيستخدم ال Ethernet Technology مع ال Fiber Channel ، بمعنى انك مش لازم تروح تشترى Dedicated Switches علشان تعمل Enable لل Fiber Channel Over Ethernet وبالتالى هو كان مهم جدا

اما بقى ال Fiber Channel فكان لازم تروح تشترى حاجة كده اسمها SAN Switches علشان تقدر تشغله

عندنا بقى ال iSCSI ، وده بقى بيستخدم ال IP Transport او بمعنى اصح بيستخدم ال IP Network العادية خالص ، يعنى بيستخدم ال switches العاديةخالص وال Interfaces العادية خالص برضو وبيستخدمهم كبروتوكول علشان يقدر يتكلم مع ال **Shared Storage Server**

وده معناه ان انت لو عندك Infrastructure موجودة ، يعنى يكون عندك مثلا سويتشات عادية خالص فانت ممكن تستخدمها علشان تشغل ال iSCSI

طيب ال iSCSI من اسمه قبل ما نتكلم عن اى حاجة ، كلمة SCSI اصلا هى اختصار ل

Small Computer System Interface

اى بقى معناها ؟؟ بكل بساطة هى اللغة او ال **Language Of Love** زى ما بتوع ال Network بيقولوا اللى كانت بتستخدم علشان لو عندك سيرفر والسيرفر ده فى disk جواه

دلوقتى بقى علشان السيرفر يكلم الديسك اللى جواه ده بشكل Locally ، اللغة دى بقى اسمها **SCSI** ، اه يبقى نفهم من كده ان دى هى اللغة اللى اى سيرفر بيقدر انه يكلم اى هارد ديسك جواه ، **طيب اى بقى ال iSCSI ؟؟**
قالك بس ان هخلى اللغة دى بقى اللى هى ال iSCSI هعملها
Transport over The Internet او Over IP ومن هنا بقى جه مصطلح ال iSCSI اللى هو اختصار ل Internet Small Computer System Interface ، وشهرته جات من انه بيستخدم ال IP Network العادية علشان يبدأ ينقل
ال SCSI Commands العادية

واصلا ال SCSI Language دى عبارة عن لغة كده علشان تكتب الداتا على الديسك وطبعا خليك فاكر انها كانت بتستخدم بشكل Locally بس

يعنى بكل بساطة هيكون عندى مثلا سيرفر عليه هارد ديسك وهوصله بسيرفر تانى ، والديسك اللى موجود على السيرفر الاولانى هيظهر كأنه Attached بالسيرفر التانى ، بس طبعا هو فعليا موجود على السيرفر الاولانى ، هنعمل ده ازاى بقى ؟ هنعمله عن طريق ال iSCSI Protocol

طبعا ال iSCSI Protocol بيتكون من جزئين ، الاول وهو ال i او ال Internet او ال IP وطبعا الجزء التانى وهو ال SCSI اللى هى الاوامر اللى هيستخدمها علشان يكتب الداتا على الديسك

يبقى ال iSCSI هيحققلى حاجة وهى ان يكون عندك ديسك Locally Attached على مكنه ويظهر كأنه Attached على جهاز تانى

طب ليه ال iSCSI مشهور كده ؟ هو مشهور بسبب انه قدر يحقق حاجات خرافية ، زى مثلا السرعات العالية بتاعت الكابلات اللى بين السيرفرات وبعضها ، وطبعا زى ما انت عارف ان intel عملت كارت ethernet سرعته 80 جيجا

والميزة التانية من مميزات ال iSCSI وهى انه مش محتاج
اى Special Infrastructure ، يعنى بيشتغل على السويتشات العادية وطبعا ده ممكن يعمل reduce لل cost ودى حاجة كويسة جدا فى حد ذاتها ان المصاريف تقل

ومتنساش ان ال iSCSI بيستخدم ال TCP Connection وال default port بتاعه هو 3260

وعندنا فى اللينكس بقى كان فى Implementation قديمة خاصة بال iSCSI ، دلوقتى بقى ال Implementation اللى هنشتغل عليها اسمها LIO ودى اختصار ل Linux Input Output

تعالى بقى ن implement ال iSCSI عندنا ، اولا هنعمل iSCSI Server هيكون عليه ال Storage وهنعمل ال iSCSI Client اللى هياخد من السيرفر ، وبالمناسبة برضو ال iSCSI Server اسمه ال **Target** وال iSCSI Client اسمه ال **Initiator** ، يبقى خليك فاكر ديما ان السيرفر هو ال **target** ديما وال client هو ال **initiator**

ممكن تجرب كده

yum search iscsi

بس طبعا ال Package مش اسمها iscsi طيب ال Package بقى اسمها **targetcli** ، يبقى انت هتسطبها على جهاز ال iSCSI Server

yum install targetcli

بعدها بقى هتلاقى فى Command Line اسمه

targetcli

اه وبالمناسبة ابقى اتأكد ان ال target.service معمول ليه loaded و active

systemctl status target.service

قبل ما تعمل اى حاجة اتأكد اصلا ان ال Backed End Storage بتاعتك شغالة ، يعنى تشوف الهاردات اللى عندك ظاهرة ولا لأ عن طريق الامر lsblk طبعا ال Backed End بتاعتك هناهى ال sdb اللى انت ضفته وهكذا يعنى

طبعا انا ممكن استخدم الهارد ده بشكل مباشر ، بمعنى انى ممكن اعمله export بشكل مباشر وممكن استخدمه ك LVM وبعدين اعمله export ، **طيب انهى الافضل انك تستخدمه مباشر ولا تستخدمه ك LVM وبعدين تعمله export ؟**

اكيد طبعا الافضل انك تستخدمه ك LVM وده لسبب مهم جدا وهو افرض ان اليوزر طلب منك انك تزود المساحة بتاعته مثلا وزى ما انت عارف ان

ال LVM فى عملية ال extend وال shrink بيكون Flexible جدا جدا ، يبقى الافضل انك تحوله ل LVM وبعدين تستخدمه او بمعنى اخر تعمله export

دلوقتى هنبدأ نحوله ل lvm عن طريق الاوامر دى

pvcreate /dev/sdb

vgcreate data /dev/sdb

lvcreate --size 10G --name oracle data

طيب افرض وانت بتعمل ال Logical Volume ظهرتلك رسالة ال error دى

Volume group "data" has insufficient free space (2559 extents): 2560 required.

اى العمل بقى هنا ؟؟ اولا انت عندك عدد ال extents ناقص لسبب ما زى مثلا انت عملت format للهارد بطريقة مش صحيحة او مثلا المساحة مش كافية

وبالتالى انت لازم تنفذ الامر ده علشان تعرف عدد ال extents اللى موجودين ضمن ال Volume Group دى عن طريق الامر

vgs -o +vg_free_count,vg_extent_count

```
[root@server ~]# vgs -o +vg_free_count,vg_extent_count
  VG     #PV #LV #SN Attr   VSize   VFree   Free #Ext
  centos   1   2   0 wz--n- <29.00g   4.00m    1 7423
  data     1   0   0 wz--n- <10.00g <10.00g 2559 2559
```

كده انت لازم وانت بتعمل ال Logical Volume تحددله عدد ال extents اللى هيستخدمها عن طريق الامر

lvcreate -l1255 -n oracle data

كده انت قولتله انه هيحجز نصف عدد ال extents اللى موجودين فى ال Volume Group اللى اسمها data ، زى كأنك برضو قولتله انك هتستخدم 10 جيجا بس ، اللى هى النصف على اعتبار ان مساحة الهارد اللى ركبناه فى ال Virtual Box هو 20 جيجا بس

تعالى بقى نعمل export لل Logical Volume اللى احنا عملناه ، اول حاجة هتكتب الامر ده بس فى الترمنال targetcli ، واول ما تفتحته هتلاقى ليه shell خاصة بيه هو

```
[root@server ~]# targetcli
Warning: Could not load preferences file /root/.targetcli/prefs.bin.
targetcli shell version 2.1.fb46
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.

/>
```

وبالمناسبة هو ليه commands زى اللى انت بتستخدمها بشكل يومى ، زى ال

ls

طيب بداية بقى ، هتلاقى ال targetcli منظم كده من جواه لشوية حاجات اول ما تكتب الامر ls مثلا

```
/> ls
o- / ..... [...]
  o- backstores ..... [...]
  | o- block ..... [Storage Objects: 0]
  | o- fileio ..... [Storage Objects: 0]
  | o- pscsi ..... [Storage Objects: 0]
  | o- ramdisk ..... [Storage Objects: 0]
  o- iscsi ..... [Targets: 0]
  o- loopback ..... [Targets: 0]
/>
```

زى ال **backstores** ، ودى عبارة عن الحاجات اللى انت عملتلها export عندك ، وبالمناسبة انت ممكن تعمل export على block device او على fileio وطبعا على pscsi او ramdisk

تعالى بقى نتكلم عن الاتنين دول اللى هما ال block device وال fileio ومعظم شغلك يكون معاهم ، طيب قولنا الاولانى علشان ت export ل block device والتانى هو ال fileio ، اى بقى ال fileio دى ؟؟ بص انا ممكن اعمل file واعمل export كانه block device لل Storage ، ازاى بقى ؟؟

استنى على رزقك دلوقتى

تعالى دلوقتى اعمل كده

cd backstores

وبعدين وانت جوه ال backstores هتلاقى الناتج كده

```
/> cd backstores/
/backstores> ls
o- backstores ..................................................................... [...]
  o- block ......................................................... [Storage Objects: 0]
  o- fileio ........................................................ [Storage Objects: 0]
  o- pscsi ......................................................... [Storage Objects: 0]
  o- ramdisk ....................................................... [Storage Objects: 0]
/backstores>
```

وتعالى برضو ادخل جوه ال block اللى موجود جوه ال backstores

```
/backstores> cd block
/backstores/block> ls
o- block ..... [Storage Objects: 0]
/backstores/block>
```

طبعا هتلاقى ان مفيش عندنا اى block devices معمول ليها exported لحد دلوقتى ، **وبالمناسبة وانت مثلا فى اى مسار هنا لو ضغطت 2 tab هيديك كل الاوامر اللى انت ممكن تستخدمها**

تعالى بقى نفذ الامر ده علشان تعمل backstore

create sql /dev/data/oracle

الامر ده معناه انى بقوله انى عايز اعمل **backstore** اسمها **sql** مثلا

او بمعنى اخر انا هعمل export ل block device اسمها

/dev/data/oracle

وطبعا هعملها export بالاسم **sql** مثلا

بس طبعا متنساش ان ال path ده لازم يكون موجود ، يعنى لازم يكون عندك block device كده

/backstores/block> create sql /dev/data/oracle
Created block storage object sql using /dev/data/oracle.
/backstores/block>

ممكن طبعا تنفذ الامر ls تانى

```
/backstores/block> ls
o- block ..... [Storage Objects: 1]
  o- sql ..... [/dev/data/oracle (5.0GiB) write-thru deactivated]
    o- alua ..... [ALUA Groups: 1]
      o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
/backstores/block>
```

كده الخطوة الاولى تمت وهى اننا عملنا export لل device ده بالاسم **sql**

الخطوة اللى بعد كده تعالى كده نرجع خالص عن طريق الامر cd واضغط على المؤشر وبعدين حرك المؤشر واختار اول واحده واضغط عليها علشان ترجع لل root بتاع ال targetcli

وتعالى نفذ ls مرة تانية

```
/> ls
o- / ..... [...]
  o- backstores ..... [...]
  | o- block ..... [Storage Objects: 1]
  | | o- sql ..... [/dev/data/oracle (5.0GiB) write-thru deactivated]
  | |   o- alua ..... [ALUA Groups: 1]
  | |     o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
  | o- fileio ..... [Storage Objects: 0]
  | o- pscsi ..... [Storage Objects: 0]
  | o- ramdisk ..... [Storage Objects: 0]
  o- iscsi ..... [Targets: 0]
  o- loopback ..... [Targets: 0]
/>
```

طبعا زى ما هو ظاهر قدامك انه بيقولك ان انت عندك فى ال backstores عندك فى ال block device اللى جواها ، انت عندك ال device دى معمول ليها export

تعالى بقى نفذ الامر ده وادخل جوه ال iscsi

cd iscsi

ولو جيت تنفذ الامر

create

وضغطت tab 2 هتلاقيه ظهرلك كلمة wwn =

/iscsi> create wwn=

اى بقى ال wwn ؟؟ طيب بداية كده ال iSCSI Server لما يحب يتكلم مع ال client هل هيتكلموا مع بعض عن طريق ال hostname ولا عن طريق اى بالظبط ؟؟ طبعا مش هيستخدموا ال hostnames ده كده غلط ، وطبعا متخلطش بين ال IP اللى هو عبارة عن بروتوكول الداتا بتنتقل عن طريقه ، بمعنى انه Transport Protocol ، لكن طبعا لما ياجوا يتكلموا لازم كل واحد فيهم يكون ليه اسم ، طبعا هما مش هيقدروا يستخدموا ال hostname العادى اللى احنا بنستخدمه فى معظم ال services التانية ، اومال هيستخدموا اي ؟؟

قالك هيستخدموا حاجة اسمها **IQN** ودى اختصار ل iSCSI Qualified Name ؟ اى بقى ال IQN ، قالك ده بقى اعتبره كأنه هو ال hostname اللى هيستخدموه علشان يتكلموا مع بعض

بيقولك بقى ان ال iQN ، هو عبارة عن name بيكون Unique للجهاز بتاعك ده ، طيب حلو ، ال syntax بتاعه بيكون كده

iqn.date.reverse domainname.servername

تعالى بقى نترجم الكلام ده ، اولا تخيل ان انت عندك سيرفر اسمه

storage.mostafa.com

يبقى اذا ال iqn بتاع ال hostname هيكون اى ؟؟

هيكون كده

iqn.date

طب استنى اى ال date ده ؟؟ عادة ال date ده بيكون هو العنوان اللى الشركة بتاعتك بدأت فيه ، يعنى مثلا لو شغال فى شركة والشركة دى اسمها test والشركة دى بدأت شهر 5 عام 2013 ، يبقى اذا الاسم بتاعك هيكون كده

iqn.2013-05

طيب وبعد كده اى بقى ال **reverse domain name** ؟ بص كده على اسم ال **server** عندك هتلاقيه **storage** ، طب وال domain name هو اى؟ طبعا هو mostafa.com

يبقى اذا الاسم هيكون كده

iqn.2013-05.com.mostafa.storage

كده نستنتج ان ال syntax هو كده

iqn.date.reverse domain name.server name

iqn ======> iqn

date ========> 2013-05

reverse domain name ======> .com.mostafa يعنى الدومين بتاعك بس طريقة معكوسة

server name =======> storage اللى هو اسم الجهاز بقى

طبعا فى ال syntax كلمة **iqn** دى ثابتة يعنى standard ، مش هينفع تغيرها

نرجع بقى لموضوعنا ، دلوقتى انا كنت داخل جوه ال iSCSI

/iscsi>

دلوقتى بقى انا عايز اعمل iqn للجهاز + انى عايز اعمل export لل device اللى هى oracle ، عن طريق الامر التالى

/iscsi> create iqn.2018-06.com.iscsi.server
Created target iqn.2018-06.com.iscsi.server.
Created TPG 1.
Global pref auto_add_default_portal=true
Created default portal listening on all IPs (0.0.0.0), port 3260.
/iscsi>

طبعا بالنسبة للdate ، انا هنا عملت اى تاريخ وخلاص ، علشان انت مش فى Production Environment

تعالى نفذ ls

```
/iscsi> ls
o- iscsi ..... [Targets: 1]
  o- iqn.2018-06.com.iscsi.server ..... [TPGs: 1]
    o- tpg1 ..... [no-gen-acls, no-auth]
      o- acls ..... [ACLs: 0]
      o- luns ..... [LUNs: 0]
      o- portals ..... [Portals: 1]
        o- 0.0.0.0:3260 ..... [OK]
/iscsi>
```

اى بقى اللى حصل هنا ، دلوقتى انا بعد ما عملت create للiqn ، اوتوماتيك فى portal تمت اضافته

```
o- portals ..... [Portals: 1]
      o- 0.0.0.0:3260 ..... [OK]
```

اى بقى ال portal ده ؟؟ بكل بساطة ، بيقولك ان ال iSCSI وهما بيعملوه ، هل تفكتر ان فيه interface وحيد هو اللى ال iSCSI بيكون connected بيه ، او عن طريقه

طيب هو اصلا عادة اى Storage Servers بيكون ليها اكتر من interface وده الطبيعى اصلا ، وكمان كل interface بيكون connected على switch مختلف وده العادى اصلا برضو

وطبعا انت ممكن تقول اننا ممكن نعمل **teaming** هنا ، هقولك لا غلط ، مش هينفع خالص ، لان هنا كل switch بيكون **standalone** كده لوحده ، فا هنا مستحيل تعمل teaming
برضو ممكن تفكر وتقول انك ممكن تعمل teaming على نفس ال switch ، هقولك طب افرض ان ال switch ده وقع ، يبقى انت كده روحت فى داهية

بالاضافة لكده ، هل انت محتاج انك تخلى ال iSCSI ي run على كل ال interfaces اللى عندك ، اكيد طبعا لأ ، لان انت هيكون عندك بعض ال interfaces بس هى اللى واصله وبعض ال interfaces هى اللى بت listen لل iSCSI

هنا بقى قالك بس انا هخلى ال interface اللى تقدر تعمل listen او بمعنى اخر انها تقدر ت serve ال iSCSI Traffic هسميها بقى Portals ، ودى عبارة عن البوابة او البوابات اللى ال iSCSI Traffic هيعدى منها ، يبقى اذا ال Portals هو عبارة عن ال IP بتاع ال Interface اللى هي Listen على iSCSI وهيستنى منه ترافيك رايحله او ترافيك جي منه

طيب لو انت ضفت على ال portal ده ال port بتاعه ، يبقى كده اسمه ال Portal Group ، نفهم من كده ان ال IP زائد ال Port الاتنين اسمهم ال Portal Group

دلوقتى بقى انت لما قولتله انك عايز تعمل export لل **iscsi** لل iqn اللى اسمه كذا ده ، راح هو اوتوماتيك قالك انه عمل default portal وكمان بي Listen على كل ال interfaces باى ديفولت by default ، وطبعا الرسالة اهى

Created default portal listening on all IPs (0.0.0.0), port 3260.

وقالك كمان انه عمل

Created TPG 1.

يعنى

Target Portal Group 1

النقطة اللى بعد كده وهى ال **acls**

o- acls ..... [ACLs: 0]

هو انت تفتكر ان السيرفر هيعمل accept لاى connection جى من ناحية ال Client ، لا طبعا ، والا لو كان اى حد يقدر انه ي Access السيرفر يبقى هياخد برضو access على ال Storage اللى موجودة دى ، طب قالك بس علشان نحل المشكلة دى ، احنا هنعمل حاجة اسمها Access Control List ، يعنى مثلا اقوله ان ال Client الفلانى ده هو الوحيد اللى يقدر يعمل connect على السيرفر ده ، طيب احنا دلوقتى هنحدد ال Client ده ازاى ؟ هل عن طريق الاسم ولا عن طريق ال IP ولا عن طريق اى بالظبط ؟قالك **هتحدده مستخدما ال IQN**

تعالى بقى نخش جوه ال acls دى ، عن طريق الامر

```
/> cd iscsi/iqn.2018-07.com.iscsi.server/tpg1/acls
/iscsi/iqn.20...ver/tpg1/acls> ls
o- acls ..........................................................................
[ACLs: 0]
/iscsi/iqn.20...ver/tpg1/acls>
```

دلوقتى هنعمل acl عن طريق الامر iqn وهو وهو نفس الامر اللى عملنا بيه iqn لل Storage Server ، الامر كالتالى

```
/iscsi/iqn.20...ver/tpg1/acls> create iqn.2018-07.com.iscsi.client
Created Node ACL for iqn.2018-07.com.iscsi.client
/iscsi/iqn.20...ver/tpg1/acls>
```

خليك فاكر الاسم بتاع ال iqn اللى انت عملته هنا فى ال acl بتاع ال client ، علشان هتحط نفس الاسم برضو عند جهاز ال Client

تعالى كده اعمل

```
/iscsi/iqn.20...ver/tpg1/acls> ls /
o- / ..... [...]
  o- backstores ..... [...]
  | o- block ..... [Storage Objects: 1]
  | | o- sql ..... [/dev/data/oracle (5.0GiB) write-thru deactivated]
  | |   o- alua ..... [ALUA Groups: 1]
  | |     o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
  | o- fileio ..... [Storage Objects: 0]
  | o- pscsi ..... [Storage Objects: 0]
  | o- ramdisk ..... [Storage Objects: 0]
  o- iscsi ..... [Targets: 1]
  | o- iqn.2018-07.com.iscsi.server ..... [TPGs: 1]
  |   o- tpg1 ..... [no-gen-acls, no-auth]
```

```
|   o- acls ..... [ACLs: 1]
|   | o- iqn.2018-07.com.iscsi.client ..... [Mapped LUNs: 0]
|   o- luns ..... [LUNs: 0]
|   o- portals ..... [Portals: 1]
|    o- 0.0.0.0:3260 ..... [OK]
 o- loopback ..... [Targets: 0]
/iscsi/iqn.20...ver/tpg1/acls>
```

كده الحكاية بقت واضحة ، انت بقى عندك block device اسمها **sql** بتشاور على **lv** اسمه

/dev/data/oracle

او بمعنى اصح انت عندك block device اسمها

/dev/data/oracle

ومعمول ليها export بالاسم **sql** ، وطبعا هيتعملها export عن طريق اى interface ، اللى هو ده

0.0.0.0:3260 ..... [OK]

وبعدين انا هستخدم ال iqn ده

iqn.2018-07.com.iscsi.server

كسيرفر

وبعدها انا هعمل export لل iqn ده

iqn.2018-07.com.iscsi.client ..... [Mapped LUNs: 0]

لل Client اللى اسمه client.server.com

دلوقتى بقى انت عندك مشكلة حقيقية موجودة ، دلوقتى انا عارف اى هى ال device اللى هيتعملها export ، بس هل انا فعليا عملتلها export بشكل فعلى ؟ طبعا لأ

وبالتالى انت لازم تعملها export تحت حاجة اسمها luns

o- luns ..... [LUNs: 0]

طيب اى بقى ال luns دى ؟ بكل بساطة السيرفر اللى عندك ده لما ياجى يعمل export لل block device عنده ، السيرفر ده او بمعنى اصح ال shared block device دى اللى هتتشاف عند جهاز ال client ، دى بقى اسمها **luns** ، ودى اختصار ل **Logical Unit Number** ، وبالتالى نستنتج من كده ان كل block device هتحتاج تعملها export ك lun

كده انا ضفت ال device ، وبالتالى معناه كأنى قولت لل block device ان انت عندك block device اهى ، بس لسه مقولتش لل iSCSI انه يعملها export ، يبقى دى كده الخطوة الاخيرة اللى ناقصاك

تعالى بقى ندخل جوه ال luns دى

/iscsi/iqn.20...ver/tpg1/luns> cd /iscsi/iqn.2018-07.com.iscsi.server/tpg1/luns

وبعدها بقى نعمل create لل lun عن طريق الامر ده

```
/iscsi/iqn.20...ver/tpg1/luns> create /backstores/block/sql
Created LUN 0.
Created LUN 0->0 mapping in node ACL iqn.2018-07.com.iscsi.client
/iscsi/iqn.20...ver/tpg1/luns>
```

شوف بقى قالك هنا انه عمل map لل node دى ، جوه ال acl ، بمعنى اخر كده انت عملت export لل block device عند ال iscsi

الشرح من تانى ، دلوقتى انت عندك ال block device دى

```
o- sql ..... [/dev/data/oracle (5.0GiB) write-thru deactivated]
```

كل ال iscsi يعرفه عنها انها عبارة عن back store ، طيب هل هى كان اتعملها export لحد الخطوة دى ، لحد ال lun يعنى ؟ اكيد طبعا لا

```
o- iscsi ..... [Targets: 1]
  | o- iqn.2018-07.com.iscsi.server ..... [TPGs: 1]
  |   o- tpg1 ..... [no-gen-acls, no-auth]
  |     o- acls ..... [ACLs: 1]
  |     | o- iqn.2018-07.com.iscsi.client ..... [Mapped LUNs: 0]
  |     o- luns ..... [LUNs: 0]
```

طيب علشان بقى تعملها export ، قالك ان عملية ال export للـ block device بالنسبة للـ iscsi اسمها lun ، خليك فاكر النقطة دى كويس ، يبقى ال device اللى بيتعملها export بيكون اسمها lun ، او logical Unit Number ، **يعنى بمجرد ما بيتعملها export بيكون اسمها lun**

طبعا لو عايزين الموضوع يكون more secure ، بمعنى ان ال client لما ياجى ياخد ال lun دى يدخل username و password

طيب تعالى نعمل ال username وال password للـ iqn بتاعت ال client ، هنروح الاول للمسار ده

```
> cd iscsi/iqn.2018-07.com.iscsi.server/tpg1/acls/iqn.2018-07.com.iscsi.client/
```

ومتنساش ايدك ديما على ال tab علشان تعرف اى الاوامر اللى متاحة ليك

هتلاقى عندك كده امر اسمه set لو ضغطت tab 2 طيب دلوقتى هنعمل user id وهنسميه ahmed مثلا

```
/iscsi/iqn.20....iscsi.client> set auth userid=ahmed
Parameter userid is now 'ahmed'.
```

وبعدها نفس الامر بس لل **password**

```
/iscsi/iqn.20....iscsi.client> set auth password=redhateng
Parameter password is now 'redhateng'.
/iscsi/iqn.20....iscsi.client>
```

كده انت ضفت ال **username** وال **password**

حلو اوى كده ، تعالى بقى نطلع من ال targetcli ، اكتب بس exit

```
/iscsi/iqn.20....iscsi.client> exit
Global pref auto_save_on_exit=true
Last 10 configs saved in /etc/target/backup/.
Configuration saved to /etc/target/saveconfig.json
```

بص كده اول ما تطلع من ال targetcli ، هو automatic بيعمل save لل confige بتاعك ده فى المسار ده فى شكل ملف json

less /etc/target/saveconfig.json

حلو كده ، دلوقتى بقى قبل ما نروح لجهاز ال Client ، فى حاجة ناقصاك وهى ، فى البداية تعالى كده نفذ

systemctl status target.service

هتلاقي ال service مش active برضو ، طيب نفذ الامر ده برضو علشان تعرف اذا كنت بت Listen على Port رقم 3260

netstat -ntlp | grep -i 3260

tcp 0 0 0.0.0.0:3260 0.0.0.0:* LISTEN -

تمام اوى ، كده انت بت Listen على البورت ده

الحاجة اللى بعد كده ، تعالى نشوف ال status بتاعت ال Firewalld

systemctl status firewalld

هتلاقيه طبعا انه active وشغال تمام ، كده انت لازم تخلى ال Firewall ، يسمح للبورت ده 3260

firewall-cmd --add-port=3260/tcp --permanent

كده احنا شبه خلصنا عند السيرفر ، تعالى بقى نروح عند ال Client

اولا قبل ما ال Client يقدر انه يعمل اى حاجة ، لازم يعمل install لل iscsi client package ، عن طريق الامر

yum install iscsi-initiator-utils

كده يبقى احنا عملنا install لل target عند السيرفر ، وعملنا install لل initiator عند ال client

حلو خالص ، دلوقتى احنا عدينا خلاص الجزء التقيل ، دلوقتى بقى قبل ما تعمل اى initiate لاى connecton او اى حاجة خالص ، خليك فاكر ديما انك محتاج تعدل ال initiator name ، فى المسار ده

vim /etc/iscsi/initiatorname.iscsi

طبعا زى ما انت فاكر ان ال initiator name هو ده

iqn.2018-07.com.iscsi.client

دلوقتى بقى تعالى نحاول نبعت Packet للسيرفر ونحاول نعمل comunicate معاه ، عن طريق الامر **iscsiadm** ، ولو انت نسيت الامر ده فا عندك ال man page بتاعته ، وهتلاقى تحت خالص فى examples

[root@client ~]# iscsiadm --mode discoverydb --type sendtargets --portal 192.168.43.19 --discover
192.168.43.19:3260,1 iqn.2018-07.com.iscsi.server

الاول تعالى اعمل enable لل service بتاعت ال iscsi عند ال client

systemctl enable iscsi.service

systemctl start iscsi

خلى بالك انك لما تيجى تعمل status لل iscsi.service هتلاقيها كده

[root@client ~]# systemctl status iscsi
● iscsi.service - Login and scanning of iSCSI devices
Loaded: loaded (/usr/lib/systemd/system/iscsi.service; enabled; vendor preset: disabled)
Active: inactive (dead)
Condition: start condition failed at Fri 2018-07-06 15:25:45 EDT; 4s ago
none of the trigger conditions were met
Docs: man:iscsid(8)
man:iscsiadm(8)

Jul 06 13:24:45 client.iscsi.com systemd[1]: Unit iscsi.service cannot be reloaded because it is inactive.
Jul 06 13:24:45 client.iscsi.com systemd[1]: Unit iscsi.service cannot be reloaded because it is inactive.

هتلاقيها انها مش active برضو

systemctl --system daemon-reload

عادى كمل ، وفكك منها ، المهم بقى بعد ما تنفذ الامر ده

```
[root@client ~]# iscsiadm --mode discoverydb --type sendtargets --portal 192.168.43.19 --discover
192.168.43.19:3260,1 iqn.2018-07.com.iscsi.server
```

وتشوف الناتج ، كده هو بيقولك انه لقى على ال ip الفلانى ده على البورت ده ، سيرفر بالاسم الفلانى ال iqn ده

وكده انت لازم تعمل start لل iscsi service الاول ، وبكده انا قادر اشوف اى اللى عند السيرفر

الخطوة اللى بعد كده ، لو جيت تعمل اى حاجة هيبقى عندك مشكلة ، والسبب انى كنت عامل authentication عند ال server ، يبقى انت كده هتعمل authenticate وتقوله انت هتستخدم انهى username و password

يعنى انت هتروح تعدل فى ملف ال configuration بتاع ال iscsi

vim /etc/iscsi/iscsid.conf

وبعدها تدور على كلمة **CHAP** ، وتعمل uncomment للسطر ده

node.session.auth.authmethod = CHAP

وكمان للسطرين دول

node.session.auth.username = username
node.session.auth.password = password

وبعدها تعمل restart لل iscsi service

service iscsi restart

وبعدين تجرب تعمل discover مرة تانية

iscsiadm --mode discoverydb --type sendtargets --portal 192.168.43.19 --discover

هتلاقيه برضو انه قدر يشوف السيرفر

طيب ملحوظة صغيرة كده ، بمجرد ما انت عملت scan لل target او حاولت انك تعمل comunicate معاه ، هتلاقى عندك على جهاز ال Client اتعمل ملف اوتوماتيك معناه انك حاولت تعمل scan لل target ده قبل كده ، فى المسار ده

less /var/lib/iscsi/send_targets/192.168.43.19,3260/st_config

يبقى اوتوماتيك هتت create ال directory الخاصة بال target ده وهيكون فيها ال config بتاعك

طيب دلوقتى بقى ال mode بتاعى مش هيكون ال discovery ، لا لا هيكون بقى ال node ، يعنى معناها انى عايز أأ attach ل node معينة ، يعنى برضو انى عايز امسك storage من node معينة

```
iscsiadm --mode node -T iqn.2018-07.com.iscsi.server -p 192.168.43.19 --login
```

دلوقتى بقى اكتب الامر fdisk -l وانت هتلاقى اضاف عندك storage جديدة اصلا او حتى lsblk

```
[root@client ~]# lsblk
NAME            MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda               8:0    0   30G  0 disk
├─sda1            8:1    0    1G  0 part /boot
└─sda2            8:2    0   29G  0 part
  ├─centos-root 253:0    0   27G  0 lvm  /
  └─centos-swap 253:1    0    2G  0 lvm  [SWAP]
sdb               8:16   0   10G  0 disk
└─sdb1            8:17   0    5G  0 part
sdc               8:32   0    5G  0 disk
sr0              11:0    1 1024M  0 rom
```

يبقى ال storage اللى تمت اضافتها هى ال **sdc**

كده انت لازم تعمل login علشان تمسك ال storage دى ، وعملية ال login معناها بكل بساطة انك كده بتمسك ال storage اللى عند السيرفر ده

لحد كده تمام اوى ، تعالى بقى نعمل reboot لجهاز ال Client بتاعتنا ونشوف اى اللى هيحصل

اولا لو جيت نفذت ال lsblk من تانى ، هتلاقى ان ال device اتعملها attach بشكل automatic اصلا

تعالى بقى عن ال Client هتلاقى فى nodes مش sendtargets المره دى ، وهيكون جواه ال node دى ال node اللى فيها السيرفر بتاعك

less /var/lib/iscsi/nodes/iqn.2018-07.com.iscsi.server/192.168.43.19,3260,1/default

هتلاقى فى عندك ملف اسمه default وفى الملف ده بقى هتلاقى عندك option مهم جدا ، وهو

node.startup = automatic

وكلمة automatic معناها هنا انه طول ما ال iscsi service شغالة وحتى لو عملت reboot للجهاز هتحاول هى تعمل attach لل storage اللى موجودة فى ال Shared Storage Server ، طبعا الملف ده فيه كل معلومات السيرفر وهو بي listen على port كام

وطبعا انت ممكن تيجى على ال storage الجديدة اللى اتضافت وتعملها format وتبدأ مثلا تعمل منها بارتيشن وتعيش حياتك بقى ، وتعملها mount برضو ، الامر اللى جى ده optionally ال tail -n 1 علشان تشوف اخر سطر بس

cat /etc/mtab | tail -n 1 >> /etc/fstab

كده بالحد الاقصى عملية ال configuration بتاعت ال iSCSI على السيرفر وال client سواء عملية التسطيب وما الى غير ذلك ، المفروض انها متتخطاش 5 دقايق

يبقى انت كده هتروح على السيرفر هتعمل اربع حاجات بالظبط ، الحاجة الاولانية بعد ما تكتب targetcli ، هتقوله فين ال block device والحاجة التانية هتحط iqn للسيرفر والحاجة التالتة اعملها map لل lun والحاجة الرابعة اعمل Access Control List ، وكده شكرا عليك ، الا بقى لو عايز تزود password g username

كده كلها اربع اوامر اللى هتعملها عند السيرفر ، والاربعة لحسن الحظ فيهم auto complete وكمان الاربعة بيبدأو بكلمة create

يبقى كده للمرة المليون خليك فاكر ان ال block device لما بيتعملها shared بيبقى اسمها luns ولا تقولى بقى lvm ولا raid ولا غيره ، وبرضو ال ip بيبقى اسمه portal

ولما بتقوله انك هتجيى عن طريق ال ip الفلانى والبورت الفلانى ده بيبقى اسمه **portal**

دلوقتى بقى لما بتضيف ال acl مع ال portal نفسه اللى هو ال ip والبورت مع ال mapped luns اللى عندك دول بيبقى اسمهم ال target portal group

من الاخر كده ، اكتب **targetcli** واكتب **ls** ،وشوف ال **tpg** بيتكون من اى بالظبط ، زى ما كأنك بتعمل lsblk وبتشوف كل partition هو جزء من انهى هارد بالظبط

بالمناسبة طبعا انت ممكن تعمل **shared fileio** ، اولا نفذ الامر ده

dd if=/dev/zero of=/root/bigfile bs=1M count=100

كده انا عايز اعمل share ل block device وال backend بتاعها عبارة عن File

تعالى بقى اكتب targetcli وادخل جوه المسار بتاع fileio

targetcli
/> cd backstores/fileio
/backstores/fileio>

وبعدين هنعمل ال block device بتاعتنا

/backstores/fileio> create myfile /root/bigfile
Created fileio myfile with size 104857600

تعالى بقى نعمل map لل block device دى ، يعنى نخلى ال client اللى اسمه
client.iscsi.com
يشوف ال block device الجديدة دى

يبقى هندخل للمسار ده

/> cd /iscsi/iqn.2018-07.com.iscsi.server/tpg1/luns
/iscsi/iqn.20...ver/tpg1/luns>

وبعدين هنفذ الامر ده

/iscsi/iqn.20...ver/tpg1/luns> create /backstores/fileio/myfile
Created LUN 1.
Created LUN 1->1 mapping in node ACL iqn.2018-07.com.iscsi.client

كده انت هتروح على جهاز ال Client وتشوف اذا كان ال device الجديدة اتضافت ولا لأ ، ولو ملقتهاش يبقى لازم تعمل logout

iscsiadm --mode node -T iqn.2018-07.com.iscsi.server -p 192.168.43.19 --logout

وبعدها تعمل login ، وتكتب بقى الامر lsblk ، هتلاقى ان الديسك الجديد ظهر ، واللى هو اصلا عبارة عن file موجود عن ال shared storage وليس block device وطبعا بقى ممكن تتعامل معاها وتعملها mount وكمان تعملها file system وغيره

وبكده كل اللى انت هتعمله عند ال Client هما 3 حاجات ، اولا هتحط اسم ال iscsi initiator name فى الملف بتاعه ، والحاجة التانية لو هتستخدم username g password يبقى تحطهم فى ملف ال iscsi.conf ، والحاجة الاخيرة هتعمل iscsi discovery وبعدها تعمل login على ال iscsi server

خلى بالك انك لما عملت logout ، وجيت عملت reboot ، هتلاقى انه عمل login automatic ، عارف ليه ؟

لان ال node اللى عند ال client اللى هو جواه ملف ال default

اللى هو بتاع ال settings ، هو ده اللى بيعمل login automatic اصلا

انما بقى لو عايز ال client ينسى كل حاجة عن السيرفر ، يبقى تستخدم ال option اللى هو delete

iscsiadm --mode node -T iqn.2018-07.com.iscsi.server -p 192.168.43.19 -o delete

3-FTP

يبقى زى ما اتعودنا ، قبل ما نتكلم عن اى **service** ، لازم نتأكد الاول من 3 حاجات ، اول حاجة وهى انك تتأكد ان ال **service** دى **installed** ، وتانى حاجة وهى ان ال **service** دى تكون **up and running** ، واخيرا تتأكد من انها هتعدى من ال **firewall** وتكون كمان **accessible** عن طريق النت

طيب تعالى بقى نروح لجهاز ال server ، وهنسطب عليه ال **vsftpd** ، ودى اسم ال Package بتاعت ال ftp service ، وهى اختصار ل **very secure ftp daemon**

yum install vsftpd

وبالنسبة لاجهزة ال client ، فانت هتعمل install ل package اسمها ftp

yum install ftp

الحاجة اللى بعد كده ، لازم تتأكد ان ال service اللى هى vsftpd دى شغالة

systemctl status vsftpd

ولو ملقتهاش شغالة ، يبقى اكيد لازم تشغلها

systemctl enable vsftpd

systemctl start vsftpd

الحاجة التالتة وهى انك تتأكد ان ال service دى accessible ، يعنى ال firewall مش عاملها block بمعنى ادق ، طيب علشان تتأكد من موضوع ال firewall ده يبقى تنفذ الامر ده علشان تعرف اى هى ال allowed ports
وال allowed services ، وطبعا لو عايز تعرف كل ال arguments اللى مع ال firewall-cmd يبقى تضغط على ال tab مرتين

firewall-cmd --list-all

services: ssh dhcpv6-client
ports:

وبعدها بقى تضيف ال ftp service ، عن طريق الامر

firewall-cmd --add-service=ftp --permanent

وبعدها تعمل reload لل firewall-cmd ، عن طريق الامر

firewall-cmd --reload

ومتنساش ديما بعد ما تكتب firewall-cmd تضغط tab 2 ، خلى بالك

services: ssh dhcpv6-client ftp
ports:

تعالى بقى نتكلم نظرى شوية ، بص بقى ال ftp عبارة عن سيرفر بيسمحلك انك ت host الملفات بتاعتك على السيرفر ، وبعد كده ال user هيعمل connect على السيرفر ده علشان يعمل download للملفات دى

طيب ال ftp بيشتغل على 2 بورتات ، هما 20 و 21 ، البورت رقم 20 ممكن تسميه كده ال control traffic ، والبورت التانى بيكون لل data transfer ، وبالمناسبة ال ftp بيشتغل على tcp connection ، يبقى خليك فاكر ان ال ftp بيشتغل ديما ببورتين ، بورت لل control والتانى لل data transfer وطبعا اسم ال Package هى **vsftpd**

طيب امتى هنحتاج ال ftp ، انت هتحتاج ال ftp لما تحب ت share ملفات للمستخدمين اللى عندك فى الشركة ، هتقولى ما انا ممكن اعمل share للملفات عن طريق ال http ؟ هقولك صح طبعا

بس ال ftp هيديك options مش موجودة عند ال http ، زى مثلا ان ال ftp بيسمحلك انك تعمل upload ل files من جهاز ال client وطبعا الحكاية دى بتم بسهولة جدا ، **بالاضافة لكده وهو ان كل user ممكن يعمل access لل home directory بتاعته عن طريق ال ftp بشكل remotely**

طيب دلوقتى بمجرد ما اتأكدت ان ال service دى up على جهاز السيرفر ، تعالى بقى على جهاز ال client واعملها test ، عن طريق الامر

ftp 192.168.43.125

وبمجرد بقى ما تشوف كلمة connected دى ، اعرف ان ال connection بينك وبين السيرفر تمام

```
[root@client ~]# ftp 192.168.43.125
Connected to 192.168.43.125 (192.168.43.125).
220 (vsFTPd 3.0.2)
Name (192.168.43.125:root):
```

مش كده وبس ، ده كمان قدر انه ي detect ال version بتاعت ال ftp وهى vsFTPd 3.0.2 ، وده طبعا البورت 220

اما بقى بالنسبة لل

Name (192.168.43.125:root):

للسطر ده ، فمعناه انه بيحاول يقولك اعمل بقى login على سيرفر ال ftp ده وطبعا بما انك اصلا وانت بتتصل بال ftp server كنت بتستخدم ال root user فا هو راح حاططهولك اذا ربما ممكن تستخدمه فى عملية ال authentication قصدى يعنى وانت بتعمل login على السيرفر

وبما انى لسه معملتش اى authentication لحد دلوقتى ، فانت ممكن تعمل login عن طريق ال anonymous user وطبعا ده ملوش اى password ، وطبعا اول ما تعمل login هيقولك انه login successful

Name (192.168.43.125:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

وبعدها ممكن تنفذ الامر ls

ftp> ls
227 Entering Passive Mode (192,168,43,125,87,12).
150 Here comes the directory listing.
drwxr-xr-x   2 0   0   6 Aug 03 2017 pub
226 Directory send OK.
ftp>

طيب سؤال بقى هو ال ftp لما بيشتغل بي serve الملفات لل users منين بالظبط ؟؟ بص هو بي serve ال files من المسار ده

cd /var/ftp/

وطبعا هتلاقى هناك directory اسمها pub ، اللى انت شوفتها لما عملت ls وبالمناسبة بقى ، لو انت حطيت اى ملف فى المسار ده ، هتلاقى كل ال users بيشوفوه

طيب لو عندك ملف وعايز تعمله download بشكل locally عندك على الجهاز ، ممكن تقوله كده

ftp> get bigfile

وانت ك system admin ، فى بعض الحاجات اللى محتاج تعملها مع ال service دى ، اول حاجة ملف ال configuration بتاع ال service دى موجود هنا

vim /etc/vsftpd/vsftpd.conf

فى الملف ده ، هتلاقى بعض ال Parameters اللى ممكن تعدلها زى مثلا ال anonymous login ممكن تخلى السطر بتاعه ك comment وبالتالى تقفل ال anonymous login او ممكن تخلى ال value بتاعته بتساوى كلمة NO وبكده انت قفلت ال anonymous login

بالمناسبة كل ال configuration اللى موجودة فى الملف ده بتكون على الشكل التالى ، بيكون عبارة عن **variable** بيساوى **value** ، وديما ديما ال value بتكون عبارة عن small letters ، وال value بتكون عبارة عن Capital Letters

وخلى بالك انك لما بتيجى تعمل comment للسطر ده مش معناه انك كده عملت disable لل anonymous login ، لان هى اصلا enabled ب by default ، كده انت لازم تغير ال value بتاعتها وتخليها NO ، حتى بص كمان على السطر ده اللى فوق كلمة anonymous

 # Allow anonymous FTP? (Beware - allowed by default if you comment this out)

allowed by default if you comment this بيقولك انها

تانى حاجة فى ملف ال configuration وهو السطر ده

local_enable=YES

ومعناه انه بيقولك هل انت عايز تخلى ال users اللى عندك يقدروا انهم ي access السيرفر ده ، اكيد طبعا ايوه ، طيب خلى بالك بقى علشان فى ملحوظة مهمة فشخ هنا وهى ان كلمة local users ، او local_enable=YES، معناها ان ال users العاديين هما اللى يأكسسوا سيرفر ال ftp وكمان ال high users ، زى ال users اللى موجودين فى جروب زى ال wheel

Name (192.168.43.125:root): ahmed
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

ملحوظة تانية مهمة ، وهى انك طالما عملت login وانت local user على ال ftp سيرفر ، دلوقتى بقى بدل ما كان بيوديك فى المسار

/var/ftp/

لا دلوقتى بقى هيوديك فى مكان ال home directory بتاعك

```
ftp> ls
227 Entering Passive Mode (192,168,43,125,21,145).
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Desktop
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Documents
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Downloads
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Pictures
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Public
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Templates
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Videos
226 Directory send OK.
ftp> pwd
257 "/home/ahmed"
ftp>
```

دلوقتى بقى من حقك انك ترفع ملفات لل home directory بتاعك ، قصدى يعنى ان كل user بيعمل login على السيرفر بيكون ليه home directory ، طيب دلوقتى انت ممكن ترفع ملفات عن طريق الامر

put bigfile

ftp> put bigfile
local: bigfile remote: bigfile
227 Entering Passive Mode (192,168,43,125,34,42).
150 Ok to send data.
226 Transfer complete.
10485760 bytes sent in 0.0711 secs (147510.16 Kbytes/sec)
ftp>

طبعا المكان اللى انت كنت واقف فيه هو ال **home directory** بتاع ال **root** وكان فيه الملف اللى اسمه **bigfile** ده

تعالى بقى روح لجهاز السيرفر

[root@server ~]# cd /var/ftp/
[root@server ftp]# ls
bigfile pub
[root@server ftp]# ls /home/ahmed/
bigfile Desktop Documents Downloads Music
Pictures Public Templates Videos
[root@server ftp]#

وخلى بالك ان ال home directory بتاع ال users اللى بيعملوا login على ال ftp server بيت create عادى على السيرفر فى المسار الطبيعى بتاع home directory اى

ls /home/ahmed

طيب نرجع بقى لملف ال configuration ، وعارف ليه انت بتقدر ترفع ملفات ، طبعا بسبب ال option ده

write_enable=YES

بالنسبة بقى للسطر ده

local_umask=022

معناه اي بقى ؟ بص هو انت لما بتيجى تعرف ملف ، الملف ده هيكون ليه permissions بالظبط ؟ اللى هيحدد الكلام ده هو ال local_umask ده انهى

وده لينك شرح ال umask

https://www.youtube.com/watch?v=JYT7y_Pe9wE&list=PLq1noKggzASu92gX_ARJRk-W9aX_4OL7d&index=7&t=0s

وفى عندك برضو ال option ده لو عايز تخلى ال anonymous users يعملوا upload لملفات

#anon_upload_enable=YES

كمان عندك برضو

#anon_mkdir_write_enable=YES

ده لو حابب ان ال anonymous users يقدروانهم يعملوا directories على السيرفر

وبصراحة بقى الملف اصلا هو self documented ، يعنى سهل فشخ انك تقرأه وتفهم اللى جواه

وفى عندك برضو ال option ده

#chown_uploads=YES
#chown_username=whoever

ومعناه انك لو عايز اى ملف يتم رفعه على السيرفر يكون مملوك لانهى يوزر بالظبط ، يعنى مين اليوزر اللى من حقه انه يشوف اى ملف على السيرفر ، بغض النظر مين بقى اللى رفع الملف ده ، يعنى اى حاجة يتعمل ليها upload تكون ملك ل mostafa مثلا

chown_uploads=YES
chown_username=mostafa

طيب انت عادة بتعمل dummy user ، يعنى user ملوش اى صلاحيات على السيرفر ، يعنى انه بيكون ليه كل الصلاحيات الخاصة بالملفات اللى بتترفع على السيرفر وبالتالى اى ملف بيترفع ، بيكون ملك لليوزر ده

بالنسبة للسطر ده

xferlog_enable=YES

معناه انك بتعمل enable لل logs بتاعت ال ftp ، طيب هى ال Logs دى هتتخزن فين بقى ، قالك هتتخزن فى المسار ده

#xferlog_file=/var/log/xferlog

وكمان ال format بتاعه ، دا لو عايز تحددله format معين

xferlog_std_format=YES

طيب هو اصلا بيستخدم ال standard format

بعد كده عندك ال option ده

#idle_session_timeout=600

وده معناه الوقت اللى لو ال User معملش اى action على السيرفر ، اوتوماتيك ال connection هيفصل ، طبعا ممكن تغير الوقت ده زى ما انت عايز

طب ليه ال idle timeout مهمة جدا بالنسبالك ، لسبب وهو انك تخيل ان انت عندك ftp server وال resources بتاعته محدودة ، طبعا انت مش هينفع تخلى ال timeout ده لملانهاية ، لان انت افرض ان يوزر عمل connect على ال ftp server ، هل هيفضل اليوزر ده فاتح session وعمال بيستهلك من ال resources بتاعت ال server

اكيد طبعا لا ، وبالتالى انت ممكن تغير الرقم 600 ده بدل ما هو 10 دقايق ، لا ممكن تخليه بس 3 دقايق او زى ما تحب يعنى

idle_session_timeout=300

وفى عندك برضو ال option ده

data_connection_timeout=120

ودى انت لازم تفعلها ، علشان اصلا معظم الناس بيعملوها ، علشان يعملوا limit لل transfer على ال ftp ، بمعنى ان انت بدل ما يكون عندك user معين ، وعمال يعمل download لملفات من ال ftp بتاعك ، لا انت تعمله
data connection timeout ، بمعنى ان انت تفصله ال connection بتاعه كل 120 ثانية مثلا

واشهر موقع لكده ، هو موقع hp ، يعنى مثلا لو جيت تنزل تعريفات من الموقع ده ، وسرعة ال download عندك بطيئة مثلا 120 KB فى الثانية ، فانت هتلاقى مثلا ال download بتاعك بيقف كل شوية ، وبتحتاج انك تعمله resume كل شوية وبالتالى هو تقريبا كده بيحاول يقلل من استهلاك ال Bandwith بدل ما اليوزر يعمل download لملفات كتيرة فشخ مرة واحدة

طبعا عندك option تانى وهو

#nopriv_user=ftpsecure

معناه انك ممكن ترن ال ftp بصلاحيات none privilege user ، بمعنى انه لو حصل attack على السيرفر ده ، فكده الهكر ده ملوش انه يعدل فى حاجة غير ملفات ال ftp بس
مع الاخذ فى الاعتبار ان الموضوع لسه فى كلام كتير خاص بجزء ال security

وفى برضو عندك option تانى وهو ان ال ftp يوقف ال abnormal connection

#async_abor_enable=YES

ممكن كمان تعمل enable لل ftp banner

#ftpd_banner=Welcome to blah FTP service.

فى عندك كمان انك ممكن تعمل deny لبعض ال users ، ولو عايز تشوف ال users اللى معمول ليهم deny ، هتلاقيهم موجودين فى المسار ده

vim /etc/vsftpd/ftpusers

طبعا ال root مش مسموح ليه انه يعمل login ، طب ليه الكلام ده ، ببساطة شديدة لان ال root ليه صلاحيات كبيرة فشخ ، وال ftp هو عبارة عن plain text protocol ، يعنى بيبعت كل حاجة non encrypted ، علشان كده من الخطر انك تخلى ال root يعمل login ، عارف حتى لو جيت تعمل login ك root هيقولك permission denied ومش هيسألك اصلا على باسورد

طيب خلى بالك وهو ان ال anonymous user محجوب بالمكان اللى هو

/var/ftp

بس ، يعنى ليه انه يتصرف فى المكان ده بس ، على عكس ال local users اللى ممكن يروحوا لاى مكان على السيرفر

خد بالك من الناتج ده

```
ftp> ls
227 Entering Passive Mode (192,168,43,125,92,169).
150 Here comes the directory listing.
lrwxrwxrwx    1 0        0               7 Jun 22 20:33 bin -> usr/bin
dr-xr-xr-x    5 0        0            4096 Jun 23 16:12 boot
drwxr-xr-x   20 0        0            3280 Jul 10 15:09 dev
drwxr-xr-x  138 0        0            8192 Jul 10 15:26 etc
drwxr-xr-x    7 0        0              73 Jun 23 14:51 home
lrwxrwxrwx    1 0        0               7 Jun 22 20:33 lib -> usr/lib
lrwxrwxrwx    1 0        0               9 Jun 22 20:33 lib64 -> usr/lib64
drwxr-xr-x    3 0        0              23 Jun 22 22:55 media
drwxr-xr-x    2 0        0               6 Apr 11 04:59 mnt
drwxr-xr-x    5 0        0              63 Jun 23 01:14 opt
dr-xr-xr-x  131 0        0               0 Jul 10 15:08 proc
dr-xr-x---    6 0        0             214 Jul 10 18:33 root
drwxr-xr-x   36 0        0            1200 Jul 10 15:26 run
lrwxrwxrwx    1 0        0               8 Jun 22 20:33 sbin -> usr/sbin
drwxr-xr-x    2 0        0               6 Apr 11 04:59 srv
dr-xr-xr-x   13 0        0               0 Jul 10 15:08 sys
drwxrwxrwt    9 0        0             248 Jul 10 17:34 tmp
drwxr-xr-x   13 0        0             155 Jun 22 20:33 usr
```

drwxr-xr-x 21 0 0 4096 Jul 10 15:26 var

drwxrwx--- 2 0 0 19 Jun 23 18:19 work

226 Directory send OK.

ftp>

طب كده بما ان ال local users هما كمان ، ليهم صلاحيات انهم يشوفوا اى حاجة موجودة على الجهاز ، وبالتالى انت لازم تحبس ال local users هما كمان يبقى تعمل uncomment للسطر ده

#chroot_local_user=YES

وبالتالى هو هيحجزهم ، بس ده مش كفاية لازم كمان تعمل uncomment للسطر ده

#chroot_list_enable=YES

علشان تقوله ان يحجم ال users اللى موجودين فى الملف ده ، وطبعا لازم تعمل uncomment للسطر ده هو كمان

#chroot_list_file=/etc/vsftpd/chroot_list

تعالى بقى نعمل list لل users اللى هيتعملهم تقييد بالمكان بتاعهم

vim /etc/vsftpd/chroot_list

طبعا الملف ده اللى هو chroot_list مش موجود اصلا ، فانت اللى هتعمله بال vim
وجوه الملف ده حط اليوزرز اللى عايز تحجمهم ، وكل يوزر هيكون فى سطر لوحده ، وبعدها طبعا تعمل restart لل service

طيب حتى انت بعد ما عملت الملف ده ، تفاجىء ان اليوزرز ليهم برضو صلاحيات انهم يشوفوا بقية ال directories اللى على السيرفر ، عارف ليه ؟؟

لان بكل بساطة ال SELinux معمول ليه enabled اصلا ، وبما اننا لسه مدرسناش ال SELinux ، كان المفروض اصلا ان الكلام ده يتعملوا allow عن طريق ال selinux اصلا

طيب خطوات حل المشكلة دى بكل بساطة كالاتى

اولا انت هتقول لل selinux انها تعمل allow للكلام ده عن طريق السطرين دول

setsebool -P tftp_home_dir 1

setsebool -P ftpd_full_access on

وبعدين هتضيف السطر ده

allow_writeable_chroot=YES

هتضيفه هنا كده بين السطرين دول

chroot_local_user=NO
chroot_list_enable=YES
 # (default follows)
allow_writeable_chroot=YES
chroot_list_file=/etc/vsftpd/chroot_list

وطبعا هتخلى السطر ده

chroot_local_user=NO

ال value بتاعته ب **NO** ، وبس كده ، وبعدها بقى اعمل restart لل vsftpd

systemctl restart vsftpd

هتلاقى ان خلاص اليوزرز العاديين ، ملهمش انهم يتصفحوا باقى ملفات السيرفر ،وليهم بس انهم يتصفحوا ملفات ال home directory بتاعتهم بس

```
ftp> ls
227 Entering Passive Mode (192,168,43,125,233,206).
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Desktop
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Documents
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Downloads
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Music
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Pictures
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Public
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Templates
drwxr-xr-x    2 1001     1001            6 Jun 23 14:46 Videos
-rw-r--r--    1 1001     1001     10485760 Jul 10 17:10 bigfile
226 Directory send OK.
ftp> pwd
257 "/"
```

فى حل تانى ، لحد ما نوصل لل selinux ، لان المشكلة دى تعتبر خازوق من خوازيق ال selinux ، والحل هو انك تعمل disable لل selinux ، عن طريق الامر

setenforce 0

بالاضافة لكده متنساش تضيف السطر ده طبعا

allow_writeable_chroot=YES

بين السطرين اللى فاتوا ، وبعدها تعمل restart لل vsftpd

من الاخر كده ال selinux كانت بتمنع ال user انه يعمل login ، طبعا الكلام ده كله بخصوص المشكلة دى

500 OOPS: could not read chroot() list file:/etc/vsftpd/chroot_list
Login failed.
ftp> exit

من الاخر برضو ال **vsftpd** ك service فيها شوية tricks بخصوص ال configuration بتاعها

اه بالمناسبة السطر ده allow_writeable_chroot=YES ممكن تضيفه بعد السطور كلها اصلا ، بالمنظر ده

chroot_local_user=NO
chroot_list_enable=YES
 # (default follows)
chroot_list_file=/etc/vsftpd/chroot_list
allow_writeable_chroot=YES

مش لازم فى النص يعنى

طيب بص بقى فى نقطة مهمة ، وهى ان حتى لو ال local users ليهم صلاحيات انهم يشوفوا باقى الملفات ، قصدى يعنى انهم يروحوا للمسار ده

cd /

فهما برضو ملهمش حق انهم يشوفوا اى اللى جوه المجلدات دى ، ودى بسبب ال selinux ، فانت كده هتضطر انك تنفذ الامر ده فى علشان تديلهم full access على كل حاجة فى السيرفر

setsebool -P ftpd_full_access 1

وده موقع redhat اللى انا جبت منه الحل

https://bugzilla.redhat.com/show_bug.cgi?id=919794

4-NFS

ال NFS هو اختصار ل **Network File Server** وكمان ال NFS هو واحد من ال Services اللى بتستخدم علشان ت share ال files بين ال Linux وال Unix ، وبالمناسبة لسنين كتيرة جدا ال NFS مكنش supported على Microsoft Windows ، لكن بداية من windows server 2008 أو 2012 بدأو انهم ينزلوا ليه support ، لكن فى الغالب مش هتلاقى حد فى Production Environment مشغل NFS على ويندوز ، لكن عادة ال NFS هو اشهر Network File System موجود حاليا فى الداتا سنترز ، طبعا لو انت شغال **VMware** فانت هتلاقى ان ال **Deployment** بتاعت ال NFS كتيرة فشخ ، وكذلك الامر برضو بالنسبة لل **KVM** ، فانت غالبا هتلاقى ان ال VMs بتكون hosted على storage معينة ، وبالتالى هتلاقى ان ال sharing بتاع ال Files حاجة من التلاتة ، يا اما **Fiber Channel** ، او يا اما **iSCSI** او يا اما بيكون NFS ، وعندك بقى واحدة من اهم المشاكل بتاعت ال NFS وهى ال High Availability ، لان ال High Availability بتاعته كانت قليلة جدا ، فانت مثلا بيكون عندك سيرفر وال client بي connect على السيرفر ده علشان يقرأ منه او يكتب data ، فا لو السيرفر نفسه وقع ، او اللينك فصل ، يبقى كده خلاص ال connection بتاعك فصل

وعلشان يحلوا المشكلة دى ، بدأوا انهم يفكروا فى حلول ليها ، وحرفيا هم بدأوا يعملوا implementation زى ال Parallel NFS وكمان PNFS

طيب تعالى نبدأ بقى ، اولا على جهاز السيرفر ، ال Package اسمها **nft-utils**

yum search nfs | grep -i utils

yum install nfs-utils

وبالمناسبة ال Package دى هتديك ال Support لل Client والسيرفر مع بعض ، طبعا زى ما ال man page بيقول ، فال NFS موجود ال support بتاعه فى الكرنال ود ه شىء منطقى جدا وبرضو نفس فكرة ال iSCSI وال LIO ، ال Implementations بتاعهم موجودة فى الكرنال

وعلى جهاز ال client هتسطب نفس ال Package دى

yum install nfs-utils

طيب نرجع بقى لموضوعنا ، زى ما قولنا ان ال NFS عبارة عن سيرفر وال Client بي connect عليه علشان يأكسسوا الداتا ، طيب ال clients دول بقى ممكن يكونوا سيرفرات تانية او اجهزة workstations تانية

ملحوظة ال NFS بي Listen على بورت كام ؟؟ الحقيقة ان ال NFS لما اتعمل من زمان مكنش فيه **dedicated port** شغال عليه ، بمعنى انك متقدرش تقولى النهارده انك هتشتغل على بورت رقم X او على بورت رقم Y ، ومش ال NFS بس ، لا دا كان فيه حاجة اسمها ال NIS اللى هى اختصار ل **Network Instrumentation Server**

وبالمناسبة ال NIS كان من اوائل
ال **Centralized Authentication Servers** اللى اتعملت ، ده بقى ومعاه ال **NFS** وشوية حاجات تانية كده ، كانوا بيعتمدوا على service اسمها **Port Map** ، اى بقى ال Port Map دى ؟؟ ال Port Map دى عبارة عن Service كانت موجودة ولما انت كنت بتشغل اى service زى ال NFS مثلا ، كانت بتروح تشوف انهى بورت فاضى وتحجزه لل service دى وبالتالى ت run ال service عليها ، كده انت ممكن تسأل ، اى العشوائية دى يعم ؟؟ طب كده ال Client لما ياجى يعمل connect ازاى هيعرف ان ال Service دى شغالة ع انهى بورت بالظبط ؟؟ هقولك لأ طبعا ، بص ال Client لما بياجى يعمل communicate ، اصلا جهاز ال Client وجهاز ال Server بيكون عليهم حاجة كده

اسمها **rpc bind** ، اى بقى ال rpc bind هى كمان ؟ هى اختصار ل Remote Procedure Call ، اى بقى اللى بيحصل هنا ، قالك بقى ان ال Client بيحاول يبعت rpc request للسيرفر فى الاول ، وبيحاولوا يكلموا بعض كده وال Client يسأل السيرفر اى هو البورت اللى شغالة عليه ال NFS او يعرف ال NFS او ال NIS كان معمول ليهم map على انهى بورت بالظبط ، وبالتالى يحاول ي connect على البورت ده بس كده ،

بس خليك فاكر ان المشكلة الحقيقية كانت ان البورتات اللى بتتحجز لل service دى كانت ديما يتكون عشوائية ، وبالتالى كان من الصعب جدا انك تحط Firewall Rule وتقوله اسمح لل Service دى ، وخليك فاكر برضو ان ال Firewall ال rule بتاعته بتكون غالبا static rule فطبعا الموضوع بيكون شاق ومتعب جدا ، فانت ممكن يكون دورك ك system admin انك تقول لل NFS وقف بقى الكلام الهبل ده كله واشتغل على static بورت علشان اقدر اظبط ال Firewall عندى

تعالى بقى نبص على ال Configuration بتاع ال NFS Server ، مبدئيا كده ال Configuration بتاع ال NFS واحد من اسهل ال Configurations اللى ممكن تشوفه بحياتك وهو عبارة عن ملف واحد موجود فى المسار ده واسمه

vim /etc/exports

بيقولك بقى الملف ده لو فتحته هتلاقيه فاضى By Default ، والسبب ان السيرفر بتاعك ب By Default مش بي export حاجة

دلوقتى بقى انا عايز اعمل export لحاجة ، بمعنى اخر انى عايز اعمل share ل directory مثلا او Folder زى ما بتوع ويندوز بيقولوا ، وبالتالى ال Clients يقدروا انهم يأكسسوه ويقرأو منه داتا او ياخدوا منه داتا

بسيطة خالص ، قالك مثلا انت هتعمل directory وليكن اسمها

/data

وانت هتعملها share عن طريق Permissions معينة ، زى

ال **read only (ro)** ، او ال **(rw)** وهكذا

تعالى بقى نجرب الكلام ده ، واول حاجة تتأكد ان ال service لازم تكون enabled و active ، طبعا الكلام ده للسيرفر وللل Client

systemctl status nfs.service

systemctl enable nfs.service

systemctl start nfs.service

فى بعض الاحيان جهاز ال **Client** مش بيقدر يشوف ال **shared directory** او ال **exported directory** ، فانت كده لازم تعمل **restart** لل **nfs**

systemctl restart nfs

ولو عايز تشوف ال Port اللى شغال عليها ال nfs ، نفذ الامر ده

netstat -ntlp

netstat ====> Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships

ntlp :

n =====> --numeric , -n
Show numerical addresses instead of trying to determine symbolic host, port or user names.

l ======> -l, --listening
Show only listening sockets. (These are omitted by default.

p ======> -p, --program
Show the PID and name of the program to which each socket belongs.

طبعا هتلاقيه شغال على بورت 2049

tcp 0 0 0.0.0.0:2049 0.0.0.0:* LISTEN -

وكمان هتلاقى عندك ال rpc شغالة هى كمان ومعاه شوية service كده

tcp 0 0 0.0.0.0:60616 0.0.0.0:* LISTEN 2690/rpc.statd

tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 2700/rpcbind

tcp 0 0 0.0.0.0:20048 0.0.0.0:* LISTEN 2701/rpc.mountd

تعالى بقى اعمل ال directory ده كمثال هنستخدمه

mkdir /data

وبعدين بقى روح لملف ال configuration بتاع ال NFS

vim /etc/exports

جوه الملف بقى هتبدأ تحددله ال directory اللى انت عايز تعملها share ، لكن قبل ما تعمل الكلام ده كله ال NFS بيطلب منك الاول انت هتشير الحاجات دى لمين بالظبط

لان انت مش هتعمل share ب read و write لاى حد كده فى الدنيا ، وبالتالى انت لازم تقوله انت هتشير الكلام ده لمين

فمثلا لو انت عايز تشير الكلام ده لاى حد ، حط * كده هنا وال asterisk دى معناها انك هشيرها لاى Network

/data *(rw)

ولو انت عايز تعملها share لاى Network ، يبقى تحط ال subnet بتاعتها ، بمعنى ان ال Syntax بتاع ملف ال Configuration بيكون كالتالى

A line for an exported file system has the following structure:

<export> <host1>(<options>) <hostN>(<options>)...

طبعا مكان ال asterisk ممكن تحط ip جهاز واحد او ممكن تحط subnet زى ما قولنا ، او ممكن تحط اسم ال host اللى هو اسم الجهاز يعنى وكمان اسم ال domain معاه بالمنظر ده

/data client.ahmed.com (rw)

او ممكن طبعا تقوله لل domain كامل بالشكل ده

/data ahmed.com (rw)

طيب تعالى نعمل share لاى حد وهيكون الملف بالمنظر ده

/data *(rw)

طبعا مفيش اى مسافة بين ال asterisk وبين ال permissions

كده انت عملت ال export ، المفروض بعدها تعمل اي بقى ؟ بص لو قولتلى انك هتعمل restart لل service ، فده يعتبر قرار سيئ جدا عارف ليه ؟؟ لان انت تخيل انك كنت بتشير directory اسمها /oracle ، وجيت ضفت directory جديدة ، عارف بقى لو جيت عملت restart لل service اى اللى هيحصل ؟؟

انت كل ال access اللى كان موجود قبل كده هيبقى مع السلامة ، فانت ممكن تعمل حركة اصيع وهى انك تنفذ ال command ده

exportfs -r

الامر ده هيخلى ال nfs يعمل reload ويشوف اى اللى اتضاف لملف ال configuration

طيب بالنسبة لل Client ، من ناحية ال Client انت اولا هتعمل حاجة كده وتشوف هل فى حاجة فى السيرفر ده تقدر انك تعملها access ، يعنى هل فى directory معينة نقدر اننا نشوفها ونأكسسها ، فانت هتنفذ الامر ده

showmount -e 192.168.1.11

بص كده هتلاقى رسالة ال error دى ظهرتلك

clnt_create: RPC: Port mapper failure - Unable to receive: errno 113 (No route to host)

بيقولك **port mapper failure** ، يعنى مش قادر يتكلم مع السيرفر ، يعنى مفيش RPC Communication ، وده معناه بكل بساطة ان ال Firewall ده عامل block لل connection ده

يبقى تعالى ضيف ال nfs

firewall-cmd --add-service=nfs --permanent

برضو لو روحت على جهاز ال Client هتلاقى رسالة ال error زى ماهى ، كده معناه ان ال NFS مش كفاية ، يبقى انت هتضيف برضو ال rpc bind

firewall-cmd --add-service=rpc-bind --permanent

برضو مازالت رسالة الخطأ دى موجودة

clnt_create: RPC: Port mapper failure - Unable to receive: errno 113 (No route to host)

طيب لو عايز تجرب انك تقفل ال firewall بتاع السيرفر وبعدين تروح تتأكد من على جهاز ال Client

systemctl stop firewalld

هتلاقى ان جهاز ال client قدر انه يشوف ال shared directory وتعالى بقى شغل ال firewall من تانى

systemctl start firewalld

وتعالى برضو ضيف لل firewall ال service اللى اسمها **mountd** ، **من غير حرف ال e علشان متتلغبطش بس**

firewall-cmd --add-service=mountd --permanent

وبعدها تعمل reload لل firewall ، واوعى تنسى انك تعمل reload لل firewall علشان حوار انك لازم تعمل reload ديما لل firewall لما تضيف service موجود من اول الاصدار رقم 7.3 فى centos و redhat ، فخد بالك ديما

firewall-cmd --reload

ولا زم تعمل restart لل nfs service ديما لو حصل اى تغيير

systemctl restart nfs

كده انت هتروح لجهاز ال Client هتلاقيه بيقولك ان فى exported directory ، وبالتالى هو قارد يشوف اللى معمول ليه shared هناك

طيب ليه بقى الحوار ده حصل لما ضفنا ال **mount daemon** ، او ال mountd ؟ ليه جهاز ال Client قدر يشوف ال shared Directory ؟

بص خليك فاكر ان ال **rpc** مش service واحدة ، دى عبارة عن طريقة للل communication علشان يقدر يشوف البورتات اللى ال service شغالة عليها

وطبعا مع ال nfs هتحتاج تعمل enable للل **rpc bind** وده علشان ال client يقدر انه ي discover السيرفر ، مش كده وبس ، كمان علشان ال Client يقدر يشوف الحاجات اللى معمول ليها mount ، يبقى انت هتحتاج ال mountd او ال **rpc mountd** ايا كان اسمها تكون accessible بالاضافة للل nfs ذات نفسها انها تكون accessible

يبقى اذا خليك فاكر ديما ان ال NFS بي allocate dynamic port وبيكون Based على ال Port Map ، وال NFS ذات نفسه محتاج اكتر من service علشان يشتغل ولو عايز تعرف ال NFS معاه كام service ، اكتب

systemctl status nfs

وبعدين اضغط مرتين على ال tab

[root@server ~]# systemctl status nfs
nfs-blkmap.service nfs-idmap.service nfs-rquotad.service nfs.service
nfs-client.target nfs-lock.service nfs-secure-server.service nfs-utils.service

nfs-config.service nfslock.service nfs-secure.service
nfs-idmapd.service nfs-mountd.service nfs-server.service

لو بصيت على ال services دى ، هتلاقى ان ال NFS معاه ال

nfs-mountd.service

ودى طبعا علشان ال Client يقدر يشوف ال mounted او يشوف
ال exported storage بالاضافة لل File Share Service ذات نفسها اللى هى
ال NFS ، دى **nfs.service**

بعدين بقى تعالى اعمل mount لل shared directory عن طريق الامر

mount -t nfs 192.168.11:/data /opt

وطبعا لو عايز تتأك انها Mounted ، يبقى تجرب الامر df -h

```
[root@client ~]# df -h
Filesystem              Size  Used Avail Use% Mounted on
/dev/mapper/centos-root   50G  4.1G   46G   9% /
devtmpfs                 984M     0  984M   0% /dev
tmpfs                   1000M     0 1000M   0% /dev/shm
tmpfs                   1000M  8.9M  991M   1% /run
tmpfs                   1000M     0 1000M   0% /sys/fs/cgroup
/dev/mapper/centos-home   47G   74M   47G   1% /home
/dev/sda1               1014M  200M  815M  20% /boot
```

Public 281G 182G 99G 65% /media/sf_Public
tmpfs 200M 0 200M 0% /run/user/0
192.168.1.11:/data 27G 4.8G 23G 18% /opt

تعالى بقى اعمله umount من تانى

umount /opt

هنرجع تانى للملف بتاعتنا ، وهنقوله اننا عايزين نعمل share ل IP معين

vim /etc/exports

/data 192.168.1.9(rw)

وبعدها تعمل

exportfs -r

وتعالى بقى عند جهاز ال client ونفذ

[root@client ~]# showmount -e 192.168.1.11
Export list for 192.168.1.11:
/data 192.168.1.1

المرة دة بيقولك ان ال directory دى معمول ليها shared للاسم ده او للجهاز اللى ال ip بتاعه كذا
طب تعالى كده اعمل mount ، هتلاقيه طلعلك الرسالة دى

[root@client ~]# mount -t nfs 192.168.1.11:/data /opt
mount.nfs: access denied by server while mounting 192.168.1.11:/data

ليه بقى لان انت حددت فى ملف ال exports جهاز واحد بس اللى هو كان ال ip بتاعه ده

/data 192.168.1.1(rw)

وبالتالى هو مش لاقى نفسه ، يبقى انت ترجع تعدل الملف وتحط ip الجهاز المظبوط ، ولو عايز تشير الكلام ده ل subnet كاملة يبقى تكتب الكلام ده

/data 192.168.0.0/16(rw)

وبعدها بقى روح لجهاز ال Client وشوف اذا كنت هتقدر تشوف ولا لا

showmount -e 192.168.1.11

وبعدها بقى اعمله mount

mount -t nfs 192.168.1.11:/data /opt

تعالى خلاص بقى اعمله umount

umount /opt

دلوقتى فى سؤال بيطرح نفسه انا لما جيت عملت share للملفات ، قصدى يعنى ان انا عندى ال client اهو قدر انه يعمل mount لل directory دى بدون اى مشاكل ، دلوقتى بقى الملفات اللى هتتكتب عن طريق ال Client هيبقى مين ال owner بتاعها ؟؟

الاول ارجع كده اعملها mount من تانى

mount -t nfs 192.168.1.11:/data /opt

وجرب تعمل ملف فى المسار /opt

touch file1 /opt

هتلاقيه بيقولك Permission Denied

touch: cannot touch ‘file1’: Permission denied

طب ليه مش قادر تكتب مع انك عامل ليها share ك rw

[root@server ~]# cat /etc/exports
/data 192.168.0.0/16(rw)

عارف ليه ؟؟ بكل بساطة بسبب ال SELinux ، تعالى كده برضو وقفها عن طريق الامر ده

setenforce 0

برضو مش هتقدر تكتب ، هيقولك برضو Permission Denied

طب تعالى برضو جرب كده

mount | grep -i /opt

[root@client opt]# mount | grep -i opt
192.168.1.11:/data on /opt type nfs4
(rw,relatime,vers=4.1,rsize=262144,wsize=262144,namlen=255,hard,proto=tcp,port=0,timeo=600,retrans=2,sec=sys,clientaddr=192.168.1.9,local_lock=none,addr=192.168.1.11)
[root@client opt]#

هتلاقى انها فعليا معمول ليها mount ك read و write ، بالمناسبة ال firewall

هنا ملوش علاقة ، احسن تقول طب ما نجرب نقفل ال firewall

طب اومال ليه بقى مش عايز يكتب جوه ال exported directory دى ؟؟

طيب تعالى تانى كده اعملها umount

umount /opt

اوبا امسك عندك ، عارف انت ليه مش قادر تكتب جوه ال directory دى ؟؟

بكل بساطة علشان ال other مش معاهم غير ال read وال execute بس

[root@server ~]# ls -ldh /data/

drwxr-xr-x. 2 root root 6 Jul 11 13:10 /data/

كده انت محتاج تغير ال permissions بتاعت ال others وتخليهم يقدروا يكتبوا

chmod o+w /data

كده المشلكة اتحلت ، ارجع بقى اعمل mount من تانى لل directory وجرب تكتب جواها هتلاقيك قدرت تكتب

وهنا انت محتاج تظبط ال permissions بتاعت ال directory قبل ما تعملها share او export الاتنين نفس المعنى

طيب تعالى بقى روح لجهاز ال Client ، واكتب ls -lh ، هتبص تلاقى الملف ات create بصلاحيات ال **nfsnobody**

[root@client opt]# ls -lh

total 0

-rw-r--r--. 1 nfsnobody nfsnobody 0 Jul 11 16:42 file1

ويا ترى بقى مين هو كمان ال **nfsnobody** ؟؟ بص يا سيدى ، دلوقتى احنا عندنا مشكلتين ، تعالى نتكلم عن المشكلة الاولى

دلوقتى الراجل اللى عمل export لل directory دى على السيرفر كان ال root ، وال user اللى عمل mount لل directory دى على جهاز ال Client كان ال root برضو

هل تفتكر بقى ان ال root اللى على جهاز ال Client هو هو نفس ال root اللى على جهاز السيرفر ولا الاتنين دول ممكن يكونوا شخصين مختلفين ؟ طيب هما اصلا فى الطبيعى هيكونوا شخصين مختلفين 😂

طيب السؤال من تانى ، تفتكر لما السيرفر يعمل export ل directory من عنده عن طريق ال root ، دلوقتى بقى لو انا اتعاملت مع ال root اللى على جهاز ال Client على انه root برضو ، هيبقى من حقه انه يتصرف فى الملفات اللى جوه ال shared directory زى ما هو عايز

وعلشان نحل المشكلة دى ، قالك ان ال NFS ب By Default هي map ال root user عند ال client ل nfs user اسمه **nfsnobody** وده عبارة عن user ملوش اى صلاحيات تماما ، ليه ؟؟ قالك علشان يتجنب ان ممكن بالغلط ال root user اللى عند جهاز ال client هو اللى يعمل mount للداتا على جهاز ال client وبالتالى هيقدر يأكسس الداتا دى من غير ما حد يقدر انه يتحكم فيه

طب افرض انا بقى شخص غلس وعايز اقول للسيرفر انه يعامل ال root اللى موجود على جهاز ال client كأنه root مش كأنه **nfsnobody**

يبقى انت هتروح لجهاز السيرفر وتعدل ملف ال exports وتضيف الكلمة دى **no_root_squash**

بعد ال permissions

vim /etc/exports

وبعدها متنساش

export -r

روح بقى لجهاز ال client وانت root وجرب تعمل ملف ، هتبص تلاقى ان ال owner بتاع الملف ده هو ال root

-rw-r--r--. 1 root root 0 Jul 11 17:06 file2

يبقى نستنتج من كده ان ال NFS هيعمل map لل root اللى موجود على جهاز ال Client ل user ملوش اى صلاحيات يعنى unprivileged user ، اسمه nfsnobody ، **بص من تانى كلمة هي map او هيعمل map ، يعنى معناها انه هيغير ال root ، كلمة map يعنى تغيير**

طب ليه هو بيغير ال root ، او ليه الحوار ده بيحصل ، لانه بكل بساطة ال NFS عايز يتجنب انه ال root اللى على جهاز ال Client ميكونش ليه نفس صلاحيات ال root اللى موجود على جهاز السيرفر ، ولو كان ليه كل ال Permissions يبقى هيتلاعب بال shared directory او ال shared storage دى زى ما هو عايز

تعالى ارجع بقى فعل ال selinux من تانى

setenforce 1

دلوقتى بقى ممكن تعمله mount بصورة دائمة وبالتالى هتحطه فى ال fstab

```
#
# /etc/fstab
# Created by anaconda on Sun Jul  8 13:58:10 2018
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/centos-root /                       xfs     defaults        0 0
UUID=6d2d4b4b-b901-435c-959e-81d00f29d969 /boot                   xfs     defaults        0 0
/dev/mapper/centos-home /home                   xfs     defaults        0 0
/dev/mapper/centos-swap swap                    swap    defaults        0 0
192.168.1.11:/data      /opt                    nfs     defaults        0 0
```

دلوقتى بقى عندنا حاجة اخيرة وهى ، هل ال File System ده اللى هو ال NFS هل بقى ال NFS ده هو Local File System ولا هو Network File System ؟؟

طيب هسألك سؤال تانى غلس شوية معلش ، دلوقتى انا لو كنت قايل لل Client روح اعمل mount من المكان ده

192.168.1.11:/data

واعمله mount هنا فى المكان ده

/opt

لل file system ده اللى هو nfs

وطبعا ال defaults هى كده

defaults 0 0

وجه بقى ال Client حاول يعمل mount ساعة ال boot فلقى السيرفر مش up اى بقى اللى هيحصل هنا بقى ؟ هيحصل خوازيق معاك 😂😂😂

هتلاقيه جابلك الرسالة المشهورة جدا فى عالم اللينكس وهى

A start job is running for ... (25s / 1min 38s)

طيب علشان نحل المشكلة دى ، ممكن نعمل حركة صايعة كده وهى اننا هنعدل ملف ال fstab تانى وهنضيف ال option ده جمب ال defaults

192.168.1.11:/data /opt nfs defaults,_netdev 0 0

طيب اى بقى ال **netdev** ؟ ده عبارة عن option ممكن تحطه وانت بتعمل mount لاى file system ، علشان تقول لجهاز ال client ان ال file system ده عبارة عن Network File System او بكل بساطة ده عبارة عن file system بيكون accessible عن طريق ال Network ، يعنى بكل بساطة لو انت مقدرتش انك تعمله mount عن طريق ال network ابقى خلاص اعمل لل mount point دى اعملها skip مش لازم تكمل يعنى

بالمناسبة المشكلة دى لو كانت مع RHEL 6 وما قبل فكان الجهاز بي fail ومكنش بي boot

طيب netdev دى هى اختصار ل network device ، يعنى device بيكون accessible عن طريق النت

وبالمناسبة برضو الكلام ده برضو مع ال iSCSI ، ابقى راجع ال **notes** بتاعك وديما ضيف ال netdev فى حالة انك هتعمل mount ل shared storage وتخليها ديما فى ال fstab يعنى لازم تضيف ال option ده علشان الجهاز لو ملقاش السيرفر يعمل skip لعملية ال mount دى

يبقى اذا سواء مع ال iSCSI او مع ال NFS او مع ال Samba او مع اى Shared File System عن طريق ال Network لازم تضيف ال option ده ، ومن الاخر كده خليها قاعدة عندك وهى انك تحط ال option ديما ، بس طبعا متجيش فى الحاجات الاساسية وترزع ال option ده كده انت هتعك

اخر حاجة خلى بالك من الملحوظة دى اللى مشروحة على موقع redhat

Warning

The format of the /etc/exports file is very precise, particularly in regards to use of the space character.
Remember to always separate exported file systems from hosts and hosts from one another with a space character.
However, there should be no other space characters in the file except on comment lines.
For example, the following two lines do not mean the same thing:

/home bob.example.com(rw)
/home bob.example.com (rw)

The first line allows only users from bob.example.com read/write access to the /home directory.
The second line allows users from bob.example.com to mount the directory as read-only (the default), while the rest of the world can mount it read/write.

وده اللينك اهو

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/5/html/deployment_guide/s1-nfs-server-config-exports

5-Apache Server

بداية كده الاباتشى يعتبر واحد من اكبر الاسباب اللى خلت اللينكس يسيطر على عالم السيرفرات فى العالم ، وبشكل عام معظم ال web servers بتشتغل على بورت 80 ولو انت شغال secure service فهتلاقيها بتشتغل على بورت 443 ، طبعا دى ال default بورتات اللى بتشتغل عليها ال web servers ، اه وبالمناسبة البورت رقم 8080 ده مش ال default port ولا هو كمان standard port

طيب ليه بقى الاباتشى عمل الشهرة دى كلها ؟؟؟ طبعا لو انت رجعت بصيت فى سنة 1998 هتلاقى ان اللى حصل ان الاباتشى فى الوقت ده هو اول واشهر ويب سيرفر هو اللى ابتكر فكرة ان يكون عندك جهاز سيرفر واحد والسيرفر ده بيقدر انه ي host مواقع كتيرة

وفى الوقت ده بقى كانت ميكروسوفت والويب سيرفر بتاعها اللى هو **IIS** كان بقى كل مكنة بيكون عليها ويب سيرفر واحد بس ، فا دلوقتى بقى لما الاباتشى جه اشتغل على جهاز واحد بقى عندنا اكتر من ويب سايت على السيرفر ، فا اى بقى اللى حصل فى سوق الداتا سنتر وقتها؟

اللى حصل ان الناس بتوع ال hosting providers اختاروا الاباتشى انه يكون ال default web server اللى موجود وطبعا ده علشان يوفروا ال resources بتاعتهم

طبعا ده لو هنتكلم على توفير عدد الاجهزة وال power cooling وليلة كبيرة سعادتك

علشان كده الاباتشى من الوقت ده لحد النهارده فضل مسيطر على سوق السيرفرات ، وطبعا لما الاباتشى سيطر بالشكل الكبير ده ، هوب ال community بتاعه كبر جدا وبالتالى اتعمله addons كتيرة فشخ ، او ممكن تعتبر كلمة addons ك modules ، يعنى اتعملت modules كتيرة للاباتشى ، زى انهم عملوا module ان الاباتشى يعمل authenticate من ال LDAP وهكذا بقى لحد ما الاباتشى كان

The Most Supported Web Server In The World

وبالتالى الاباتشى لما المجتمع بتاعه كبر ، بقى بي support لغات كتيرة جدا زى ال **PHP** وال **Perl** وال **Ruby** وال **Python** ، يعنى تقريبا كده اى حاجة كانت بتعدى عليه كان بيقولك انه بيديك support ليه ؟ طبعا لان ال community بتاعه كبر جدا

طيب خلينا نتكلم بشكل واقعى اكتر بقى ، الاباتشى لما كبر واتشهر بالمنظر ده بقى عامل زى الكائن الكبير اوى ، وبقى عامل بالظبط زى شخص كل ما يلاقى قدامه اى نوع اكل يروح يجرى ياكل فيه ، فا اى بقى اللى حصل ؟؟

اللى حصل انه تخن اوى وكبر اوى ، فانت دلوقتى علشان تتيون الاباتشى ده (تت tune) تتيون يعنى تظبط الاباتشى ، طيب انت علشان تظبط الاباتشى ده حاول تعرف اى اللى انت محتاجه منه بالظبط ، لانه زى ما قولنا ان الاباتشى دلوقتى بي support اى حاجة ، وحتة انه يدعم اى حاجة فى نفس الوقت ده يعتبر ميزة وعيب فى نفس الوقت ، لان انت لو عملت install للاباتشى وعملت كمان install لكل ال support packages معاه كده انت لبست نفسك ووديت نفسك فى 60 داهية ، طب ليه بقى ؟؟
لان انت تخيل ان انت عندك ويب سايت web site مكتوب بالبايثون مثلا ، وجيت انت عملت install للاباتشى وعملت install كمان لل php modules معاه كده انت وديت نفسك فى مصيبة سودة

ليه برضو ؟؟ لان افرض انهم اكتشفوا اى Vulnerability لل php وحتى لو انت مش بتستخدم ال php فانت برضو عرضت نفسك للخطر ، وبالتالى انت لازم تعرف انت عايز اى بالظبط من الاباتشى

ودى تعتبرها قاعدة ثابتة معاك وانت شغال مع الاباتشى ، بمعنى اخر انك متحاولش انك تعمل install لحاجة انت مش محتاجها مع الاباتشى ، يعنى اختار ال Packages اللى انت عايزها بس

طيب تعالى بقى نعمل install للاباتشى على جهاز ال server عن طريق الامر

yum install httpd

وبعدها طبعا

systemctl status httpd

systemctl enable httpd

systemctl start httpd

systemctl status httpd

طيب فى معلومة هنا وهى ان الاباتشى على RedHat واى distro بقى based على RedHat هتلاقى اسمه httpd ، انما بقى فى Ubuntu او debian فال Package اسمها **apache2**

طبعا هو اسمه apache2 لانه اتعمله كتابة من ال scratch ، طيب بالمناسبة كمان ، هتلاقى عندك group من ال Packages اسمها basic web server

yum groups list

طيب الاباتشى لوحده كده بيقولوك انه بيديك support للملفات اللى مكتوبة HTML بس

لو جيت تنفذ الامر

yum search apache | less

اتفرج بقى على كمية ال Modules اللى بتيجى مع الاباتشى لوحده وطبعا كل scripting Language بيكون معاها Modules كتيرة فشخ ، يعنى مثلا

yum search php | less

هتلاقى ان ال php معاها modules كتيرة

طيب دلوقتى احنا عملنا install للاباتشى وبالتالى الاباتشى هي server الملفات بتاعته من المكان

ls /var/www/html

وده المكان اللى الاباشتى بي server الملفات للمستخدمين من خلاله

دلوقتى علشان اليوزر يقدر انه ياكسس المكان ده ، يبقى لازم ال firewall يسمح بكده

firewall-cmd --add-service=http --permanent

وبعدها كالمعتاد لازم تعمل reload لل firewall

firewall-cmd --reload

ممكن تروح على ال browser وتجرب ال apache عن طريق انك تكتب ال ip بتاع الجهاز

201.201.0.6

وهتلاقى صفحة Testing ظهرتلك كده ، طب الصفحة دى لازمتها اى ؟ لازمتها انها تخليك تتأكد ان الاباتشى بتاعك موجود وكمان up and running ، والصفحة دى بتيجى لما ميكونش فى ملفات معمول ليها host فى المسار

ls /var/www/html

بمعنى انت ممكن تروح للمسار ده

cd /var/www/html

وتاخد الكود بتاعك اللى انت كاتبه وتحطه فى المكان ده ، انما لو مش حاطط اى حاجة هيديك صفحة ال Testing دى

تعالى بقى مثلا اعمل صفحة index.html ، هتلاقى ان صفحة ال Testing اختفت وظهرت بدالها صفحة ال index.html ، **طب ليه او اشمعنى الصفحات بالاسم index هتعرف كمان شوية**

وملفات ال Configuration بتاعت الاباتشى بتكون فى المسار ده

cd /etc/httpd

وبالنسبة لملف ال configuration الرئيسى بتاع الاباتشى هتلاقيه موجود فى المسار ده

vim /etc/httpd/conf/httpd.conf

هنا بقى ملف ال **configuration** بتاع الاباتشى متقسم لاجزاء ، واول جزء هنتكلم عنه وهو الجزء الخاص بال **main server**

اى بقى ال main server ؟ بص خليك فاكر ان الاباتشى ممكن ي host اكتر من ويب سايت على نفس السيرفر ، فانت هيكون عندك جزء خاص بال main site يعنى بالموقع الرئيسى وهيكون عندك جزء تانى خاص باى ويب سايت تانى ، وال web sites التانية بنسميها ال **virtual hosts**

يبقى اذا جزء ال Configuration الاول هيكون خاص بال main site ، اللى هو الموقع الاساسى ، اللى هو بيتعمله host فى المسار

var/www/html

وعندنا اول حاجة بقى فى ملف ال configuration بتاع الاباتشى هو السطر ده

ServerRoot "/etc/httpd"

وده معناه ان بيقولك فين ملفات ال configuration بتاعت الاباتشى

فى بعد كده السطر ده

Listen 80

اللى هو بيقول للاباتشى انت هت listen على بورت كام بالظبط

الحاجة اللى بعد كده هتلاقيه الجزء الخاص بحاجة اسمها Dynamic Shared Object ، اى بقى ال dynamic shared object ده ؟؟

طيب الاول هتلاقى فى directive كده هتشد انتهابك اسمها include ، السطر بتاعها اهو

Include conf.modules.d/*.conf

اى بقى موضوع include ده ، بص بدل ما يخلى طول الملف بتاع الاباتشى 30 ولا 40 متر ، قصدى يعنى عدد السطور بتاعته كبيرة فشخ ، قالك لأ انا اى حاجة هحب اضيفها فى الملف ده هنادى عليها عن طريق الامر include والملفات اللى هتنادى عليها موجودة فى المسار

conf.modules.d/*conf

طيب تعالى كده افتح اى ملف من اللى موجودين فى المسار ده

vim /etc/httpd/conf.modules.d/00-base.conf

الملفات دى بقى هى عبارة عن الملفات اللى بتعمل load لل modules الخاصة بالاباتشى ، طبعا فى كل ملف هتلاقى كمية modules كتيرة فشخ بيتعملها load

وطبعا كل module او كل مجموعة modules بتعمل حاجة معينة

طيب نرجع بقى لملف ال configuration الرئيسى بتاعتنا ، ونخلينا فاكرين ان الاباتشى لما يحب ينادى على configuration معين هيعمله include ويريح دماغه

بعد كده بقى فى ملف ال configuration بتاع ال apache هتلاقى عندك السطر ده

User apache
Group apache

وده ال user اللى هيرن الاباتشى وطبعا الجروب اسمها برضو اباتشى

تعالى بقى نتكلم عن ال **Main Server Configuration**

 # 'Main' server configuration

بص الاباتشى عندك متقسم ل 3 اجزاء ، فى عندك حاجة اسمها ال

Global Configuration

وبعدين فى حاجة اسمها ال

Main Server Configuration

واخيرا عندك ال

virtual hosts configuration

اول حاجة بالنسبة لل global configuration فال settings اللى هتلاقيها فى ال global configuration بسيطة جدا زى مين ال user اللى هيشغل الاباتشى ومين الجروب بتاعته واى البورت اللى هي listen عليه واى كمان ال modules اللى بيعملها load ، يبقى دى الحاجات اللى هتأثر بشكل عام على الاباتشى سواء بشكل Main Server او بشكل Virtual Hosts

تانى حاجة ال Main Server هيكون فيها ال Configuration الخاص بالملفات اللى هيعملها serve فى المسار

var/www/html

اما بقى ال virtual hosts فانت اللى هتعمل define لل virtual hosts بايدك كمان شوية ، يعنى من الاخر كده لسه لحد دلوقتى معندناش اى virtual hosts ، بمعنى اننا لسه هنعرف ال virtual host هتبقى فين بالظبط او هتعمل serve للملفات بتاعتها منين بالظبط ، اهدى على رزقك😀

طبعا الجزء اللى احنا بصينا عليه كان الجزء الخاص بال Global Configuration تعالى بقى دلوقتى بنص على الجزء الخاص بال Main server

واول سطر configuration فى ال Main Server هو السطر ده

ServerAdmin root@localhost

اى بقى ال ServerAdmin ده ؟ ببساطة شديدة اكيد انت جربت تفتح اى web page بتاعت اى موقع مثلا وقالك مثلا انه مش قادر يعمل load للموقع ده وراح تحت كده وقالك

please contact ServerAdmin

وراح حاططلك الايميل بتاعه فانت هنا بقى ممكن تغير ال ServerAdmin وتخليه مثلا بالشكل ده

ServerAdmin support@ahmed.com

علشان تظهر فى حالة ان فى errors فى عملية ال Load بتاعت الصفحات

بعد كده هتلاقى ال directive دى وهى خاصة باسم السيرفر

#ServerName www.example.com:80

طبعا انت هتعمل uncomment للسطر ده ، بس بص كده هو هنا محدد ان البورت رقمه هيكون 80 ، طب ما احنا اصلا عرفنا الكلام ده فى ال global configuration فوق ، وبالتالى انت ممكن تمسح رقم 80 ده ، وطبعا انا ممكن ادى للسيرفر بتاعى اسم بالمنظر ده

ServerName www.ahmed.com

والاسم ده هو اسم الموقع بتاعك اللى اليوزر لما يكتبه فى المتصفح هيطلعله الموقع بتاعك

اه وبالمناسبة طبعا لازم ال domain ده اللى هو ahmed.com لازم يكون موجود على ip ، وبالمناسبة الحتة دى بتعتمد على جزئين
الجزء الاولانى عند السيرفر وهى ان انت تعرف ال hostname او بمعنى اخر ال Servername اللى هو ahmed.com

والجزء التانى عند ال Client وهو ان ال Client يقدر انه يعمل resolve لل hostname ده ، طيب هو فرضا ان ال Client بيحاول انه يعمل Access للويب سايت ده ، بس ال client ذات نفسه مش قادر يعمل resolve ، يبقى هيوصل ليه ازاى بقى اساسا وخليك فاكر ان انت المفروض يكون عندك DNS Server وال dns server ده هو اللى هيعمل resolve للاسم ده

طيب نرجع بقى لموضوعنا ، فاكر لما عملنا ال chroot environment مع ال FTP علشان الناس ميتفسحوش فى السيستم صح ؟

هنا برضو هتلاقى حاجة اسمها ال Deny access ؟ اى بقى ال Deny access دى ؟
هنا بقى مع الاباتشى برضو بيقولك انه هيعمل deny access لل directory اللى هى ال / اللى هى بمعنى اخر ال root file system وطبعا بيقولك كمان هنا انه مش هي override اى options خالص ، يعنى بكل بساطة انا بخلى الاباتشى يعمل deny لل file system كله ، بمعنى اخر انى بقول لل apache امنع اى access لل file system

```
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
```

```
<Directory />
    AllowOverride none
    Require all denied
</Directory>
```

طبعا بعد ما بتعمل deny للل file system كله ، بتيجى بقى تحت وتعمل allow للمكان ده بس اللى هو ده

```
# Further relax access to the default document root:
<Directory "/var/www/html">
    #
```

طبعا برضو عندك السطر ده

```
DocumentRoot "/var/www/html"
```

وده معناه المكان بتاع الملفات اللى انت هتعملها server منين بالظبط

بعد كده بقى قالك ان ال directory دى اللى هى var/www/html هعملها allow بالشكل ده

```
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>
```

نرجع بقى تانى لموضوعنا ، وهى ان ال directory اللى اسمها

/var/www/html

هتلاقى معاها option كده اسمه Indexes

```
# Further relax access to the default document root:
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks
```

وال Indexes دى ، عبارة عن ان مثلا لو عندك صفحة index.html فالصفحة ال index دى بتكون هى الصفحة الرئيسية للموقع بتاعك

وبيكون معاها option اسمه FollowSymLinks اللى هو اختصار ل Follow Symbolic Links ، يعنى اى بقى ؟ معناه ان انت لو عملت softlink لملف هيخلى الاباتشى يروح وراء الملف ده علشان يعمله serve هو كمان

بعد كده السطر ده

AllowOverride None

يعنى هل فى اى option عايز تعمله override ؟ اكيد طبعا لأ

وبعدها السطر ده

Require all granted

وده معناه ان ال access لل directory دى granted يعنى مسموح بيها

بعد كده بقى فى حاجة اسمها ال directory Index ودى معناها انه هيبص بس على الملفات اللى اسمها index

```
<IfModule dir_module>
   DirectoryIndex index.html
</IfModule>
```

طبعا انت ممكن تضيف اكتر من DirectoryIndex بالشكل ده

```
<IfModule dir_module>
    DirectoryIndex index.html index.php
</IfModule>
```

طبعا بعد ما تعدل اى حاجة فى الملف ده لازم تعمل restart لل httpd

```
systemctl restart httpd
```

وحط فى اعتبارك ان ال php لازم تكون متسطبة وده فى حالة انك عايز تشغل ملفات ال php

وبالمناسبة كمان الترتيب ده مهم جدا ، يعنى انت هنا بتقوله روح دور الاول على الملفات اللى بالامتداد index.html ولو ملقتهاش روح شوف الملفات اللى بالامتداد index.php وهكذا بقى

تذكر

cd -

ده بيرجعك لاخر مجلد انت كنت فيه

فى بقى عندك حاجة اسمها **htaccess** و **htpassword** اللى هو معناها ان الاباتشى بيعمل deny لل htpassword files ودى لسه هنجيلها بعدين

```
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<Files ".ht*">
   Require all denied
</Files>
```

ودى عبارة عن ملفات بتستخدمها علشان تعمل secure للاباتشى ، وزى مثلا انك لو عايز تعمل protect ل directory معينة زى مثلا انك تحطلها username و password ، والجزء ده لوحده عليه lap خاص بيه

بعد كده ال errorlogs ، اللى هو المكان اللى فيه ال logs بتاعتك

ErrorLog "logs/error_log"

وده المكان اللى فيه ال logs بتاعت ال httpd

less /var/log/httpd/

هنا بقى هتلاقى ملفين الاول هو

less /var/log/access.log

والملف ده هيكون جواه مين اللى عمل access على السيرفر بتاعك وعمله access من انهى ip بالظبط

وفى بقى عندك ملف ال log التانى وهو

less /var/log/httpd/error_log

وده بقى خاص بال errors الخاصة بالاباتشى

بعد كده بقى فى ملف ال configuration بتاعت الاباتشى ، هتلاقى كمان شكل ملف ال log عامل ازاى

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

بيكون بالمنظر اللى انت شايف ده

يعنى مثلا ال **h%** دى معناها ان هيبدأ يكتب فى الملف اول حاجة ال host بتاع الجهاز اللى عمل access على السيرفر بتاعك ، وده مثال على كده

201.201.0.2 - - [22/Jul/2018:13:09:58 -0400] "GET / HTTP/1.1" 403 4897 "-" "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:61.0) Gecko/20100101 Firefox/61.0"

بعد كده انت عندك module بالشكل ده اسمه mime

IfModule mime_module>

وهنا بقى الاباتشى بيحاول يعمل detect لل extension بتاعت الملفات اللى بيعملها serve وبيعرض كل ملف بالايقونة بتاعته ، يعنى مثلا لو فى فديو يبقى هيعرضلك ايقونة الفديو ولو في ملف pdf هتلاقيه automatic عرضلك الملف وجمبه كده ايقونة خاصة بيه ك pdf

6-Virtual Host

طبعا زى ما قولنا ان ال configuration بتاع الاباتشى بينقسم ل 3 اقسام ، اول حاجة وهى ال global configuration ودى كل وظيفتها انها بت define ال global settings اللى هى ال settings اللى بيتم تطبيقها على اى حاجة فى الاباتشى سواء كنت بتتكلم على ال main host او بتتكلم على ال virtual host او على اى حاجة تانية

والجزء التانى طبعا هو ال Main Server Configuration ، وطبعا الجزء التالت هو ال virtual host configuration

احنا المرة اللى فاتت كنا اتكلمنا عن ال Global Configuration وال Main Server Configuration ، النهارده بقى هنبدأ نتكلم عن ال virtual hosts وازاى نعمل enable لل user directories ، تعالى بقى افتح ملف ال configuration من تانى

vim /etc/httpd/conf/httpd.conf

هتلاقى عندك كده فى اخر الملف خالص خالص السطر ده

 # Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf

طبعا هنا بيقولك انه عايز يعمل include لاى حاجة موجودة فى المسار ده conf.d/*.conf ، زى ما انت عارف انه كده وفر عليك بدل ما تعمل ملف كبير ويكون فيه سطور كتيرة فشخ لا هنا هو بيقولك ان اى ملف فى ال directory اللى اسمها conf.d ويكون امتداده .conf ابقى اعمله include بقى فى ملف ال configuration بتاع الاباتشى

طيب فى حاجة عايز اقولك عليها وهى ان اى حاجة موجودة فى ال directory دى زى ما اتفقنا انها كأنها اتضافت للملف الرئيسى بتاع ال configuration

هنا بقى فى سؤال دلوقتى بقى الملفات دى لما يتعملها include الترتيب بتاعها هيكون اى بالظبط ؟ قالك ان الترتيب بتاعها هيكون ترتيب ابجدى يعنى لو عندك ملفين واحد بيبدأ بحرف ال a والتانى بحرف ال m فالملف اللى بيبدأ بحرف ال a هو اللى هيتعمله load الاول ، علشان كده يفضل انك لو بتعمل ملف configuration خاص ب virtual host او حتى خاص بيك ، يفضل انك ترتبها ترتيب ابجدى

وكمان يفضل جدا جدا ان ملفات ال configuration اللى انت هتعملها يكون الاسماء بتاعتها بالشكل ده

01-test.conf

بحيث ان عملية ال trouble shooting تكون سهلة عليك وترتبها كمان ترتيب ابجدى

تعالى بقى ندخل ال directory دى ونشوف اى اللى موجود جواها

cd /etc/httpd/conf.d

هتلاقى جواها الملفات دى

autoindex.conf README userdir.conf

لو جيت مثلا بصيت على ال userdir.conf

vim userdir.conf

ال userdir.conf ده عبارة عن module بيسمح للاباتشى انه ي serve ال http requests اللى هى ال http content بمعنى اخر من ال home directories بتاعت ال users

دلوقتى بقى تعالى مثلا واحنا على جهاز السيرفر نختار user معين من ال users اللى عندنا ونجرب عليه وليكن مثلا اسمه ali واللى اسمه ali ده عايز ي host ال http content بتاعه
طيب ال module ده اصلا ب by default هو disabled فانت بقى هتفتح الملف ده تانى

vim userdir.conf

وهتيجى على السطر ده وتغير كلمة disabled وتشيلها وتقوله انت هتعمل serve من انهى مكان بالظبط

```
UserDir disabled
```

ولو انت بقى خليت اسم ال directory دى بالشكل ده public_html

```
UserDir public_html
```

فاهتلاقيه هو اصلا تحت شوية فى الملف هتلاقيه عاملك directory statment وبيقولك ان اى حاجة موجودة فى المكان

```
<Directory "/home/*/public_html">
```

اى حاجة موجودة فى ال

/home

وبعدين اسم ال user وبعدين اسم ال directory اللى هى public_html راح بقى عاطيله options بالشكل ده

```
    AllowOverride FileInfo AuthConfig Limit Indexes
    Options MultiViews Indexes SymLinksIfOwnerMatch
IncludesNoExec
    Require method GET POST OPTIONS
</Directory>
```

المهم انى بكل بساطة كده انا سمحت للاباتشى انه ي serve ال directory اللى اسمها public_html ، طب هو انا اصلا كنت لازم اسمح للاباتشى انه ي serve من ال directory اللى اسمها public_html دى اللى هى موجودة اصلا لكل user عندى ، وطبعا زى ما انت عارف ان ال * معناها كل ال users ، هل بقى انا كنت لازم اسمح لل dir بكده ؟

ايوه طبعا ، ولو رجعت تانى لملف ال Main Configuration

vim /etc/httpd/conf/httpd.conf

كنت هتلاقى عندك directive بسيطة جدا وهى

```
<Directory />
    AllowOverride none
    Require all denied
</Directory>
```

شايف بقى ال directory دى اللى اسمها / ، كان بيقولك عليها Require all denied ، ودى بكل بساطة بتخلى الاباتشى انه يعمل deny لاى access على ال File System

يعنى حتى لو انت كنت عملت enable لل module ده اللى هو **userdir.conf** من غير ما تقوله انا لما اعملك enable انت المفروض ت serve انهى directories بالظبط ، عمر الاباتشى ما كان هيقدر انه يقرأ اى file من على ال file system من غير ما تحددله المكان اللى هيقرأ منه ده ، يبقى كده ب By Default الاباتشى بيعمل deny لاى حاجة على ال root file system ما عدا الاماكن اللى انت هتقوله انه يعملها serve وهنا بقى بالنسبة لل block دى directory

```
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>
```

انا بقول للاباتشى Require all granted يعنى انا بسمحلك يا اباتشى انك تقرأ من المكان ده اللى اسمه var/www/

وبالمناسبة انت علشان تعمل حاجة زى كده ، فا انت هترجع تانى للملف اللى هو userdir.conf وقولت للاباتشى ان المكان ده

<"Directory "/home/*/public_html>

ابقى اعمل منه serve ، طبعا لو انت كنت عايز ان الاباتشى يعمل serve للملفات ل user معين ، كنت اكيد هتشيل ال * وتكتب اسم ال user

خلاص كده احنا عملنا enable لل module ده وقولنا للاباتشى على المكان اللى هيعمل منه serve للملفات ، كده احنا جاهزين ، دلوقتى بقى تعالى غير ال shell وروح لل user اللى اسمه ahmed ده

su - ahmed

كده بقى المفروض ان ال user ده اللى اسمه ahmed يكون بيقدر انه يعمل directory ويسميها بالاسم public_html زى ما موجود فى ملف ال configuration

mkdir public_html

وتعالى برضو ندخل جوه ال directory دى

cd public_html

واعمل ملف

vim index.html

اكتب بقى اى حاجة جوى الملف ده وبعدين ارجع تانى ، وابقى اتأكد ديما ان ال directory اللى هى ال public_html ال **others** معاهم ال read وال execute permissions

drwxrwxr-x. 2 ahmed ahmed 24 Jul 24 15:59 public_html

طب ليه ؟ لان بكل بساطة الاباتشى محتاج انه يقرأ ال directory دى وال execute معناها انه يدخل جوه ال directory دى

فى حاجة تانية كده زى الخازوق انت مش واخد بالك منها وهى ، تعالى كده اعمل

ls -lh /home

drwx------. 6 ahmed   ahmed   142 Jul 24 15:59 ahmed

بص كده هتلاقى ان ال others مش عندهم اى permissions خالص على ال directory اللى اسمها ahmed دى

تعالى بقى ادى لل others صلاحيات ال execute ، وطبعا ال others هنا هما اى user تانى بما فيهم الاباتشى ذات نفسه

chmod o+x /home/ahmed

كده انا خلصت خلاص ، تعالى بقى اعمل restart للاباتشى

systemctl restart httpd

تعالى فى المتصفح واكتب فوق

201.201.0.6/~ahmed

وشايف انت علامة التلدا دى ~ معناها كلمة home directory

وهوب هتلاقي طلعلك رسالة ال error دى

Forbidden

You don't have permission to access /~ahmed/ on this server

والمشكلة دى ظهرتلى لان ببساطة عندى ال selinux معمول ليها enabled ،
تعالى كده شوف ال status بتاعت ال selinux عن طريق الامر التالى

sestatus

هتلاقيها انها enforcing وده معناها انها بتحمى السيستم عندك

SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 31

دلوقتى بس مؤقتا هوقف ال selinux عن طريق الامر

setenforce 0

وتعالى بقى جرب تانى فى المتصفح

http://201.201.0.6/~ahmed/

هتلاقيه فتح معاك

دلوقتى بقى نرجع لموضوعنا ونروح تانى للمسار ده

cd /etc/httpd/conf.d/

هتلاقى برضو هنا ملف او module اسمه manaual.conf ، ود عبارة عن ال manual configuration اللى انت ممكن ترجعله او تخليه اصلا كمرجع ليك لو انت حابب تعمل configuration معين للاباتشى بس ناسى ازاى ، ممكن تروح للملف ده وتاخد منه copy و paste ، وطبعا ده اصلا عبارة عن Package بتتسطب بالامر ده

yum install httpd-manaual

وال Manaul ده اتعمله install فى المكان ده

/usr/share/httpd/manual

تعالى كده روح للمسار ده

vim /usr/share/httpd/manual/

هتلاقى جوه ال directory دى الملفات دى كلها

bind.html expr.html license.html sections.html
BUILDING faq/ logs.html server-wide.html
caching.html filter.html misc/ sitemap.html
configuring.html glossary.html mod/ socache.html
content-negotiation.html handler.html mpm.html ssl/
convenience.map howto/ new_features_2_0.html stopping.html
custom-error.html images/ new_features_2_2.html style/
developer/ index.html new_features_2_4.html suexec.html
dns-caveats.html install.html platform/ upgrading.html
dso.html invoking.html programs/ urlmapping.html
env.html LICENSE rewrite/ vhosts/

ودى عبارة عن الملفات الخاصة بال manual بتاع الاباتشى كله

ولو عايز فى المتصفح تروح لل manual directory ده عن طريق

http://201.201.0.6/manual/

هتلاقى بقى فى ال manual ده كل ال configuration بالتفصيل اللى ممكن تحتاجه

تعالى بقى نتكلم عن الجزء الخاص بال Virtual Hosts

ازاى بقى اقدر انى اخلى الاباتشى عندى ي serve اكتر من web site ؟ بص الموضوع بسيط جدا ، اولا دلوقتى احنا هنضيف ملف configuration فى ال directory اللى اسمها conf.d ، تعالى بقى اعمل ملف configuration وسميه مثلا كده

vim 01-vhost.conf

وده هيكون خاص طبعا بال virtual hosts

دلوقتى بقى الاباتشى ممكن يديك virtual hosts باكتر من طريقة ، الطريقة الاولى اسمها ال name based virtual hosts والطريقة دى بسيطة جدا وكل فكرتها قايمة على ان الاباتشى بتاعك هيسمح انه يكون فى اكتر من web site يتعملوا serve من نفس المكنة بس لما تيجى تعمل serve هيبص على الاسم بتاعهم المطلوب اى

يعنى مثلا لو انت طلبت من السيرفر الموقع اللى اسمه www.ahmed.com ، السيرفر ده بقى هيخلى الاباتشى ي serve من directory معينة وكذلك الامر لو طلبت من نفس السيرفر الموقع www.ali.com برضو هيخلى الاباتشى ي serve من directory تانية معينة ، وده معناه ان كل web site هيكون ليه directory خاصة بيه وهيكون فيها بقى ملفات ال HTML او ال PHP الخاصة بالموقع ده

يبقى كده الاباتشى هيستخدم نفس ال IP Address ونفس ال Interface اللى ال connections جاية من عليه ، بس طبعا هيفرق بين ال web sites دى عن طريق ال name بتاعهم
يعنى هيشوف ال name اللى جايله اى بالظبط وهيقول لل user انه هيعمله serve من ال directory المعينة دى بناءا طبعا على ال Configuration بتاعت الاباتشى

والطريقة التانية هى ال ip based virtual host والطريقة دى بسيطة جدا جدا هى كمان ، والطريقة دى بتفترض ان لو ال user جاى ل ip address معين فالاباتشى هيعمل serve من directory معينة ، والحقيقة ان الطريقة دى ممتازة جدا وكمان التطبيق بتاعها بيكون سهل وابسط فى ال Local Environment ، وطبعا مش بتكون Flexible اوى فى ال Public Environments

وده لان ال Public IP Address عددها قليل جدا ، فتخيل مثلا ان انت عندك 10 virtual hosts ، فانت كده محتاجلهم 10 Public IP Addresses وطبعا الكلام ده مش Practical اوى فى ال real world ومش Practical اساسا ، فطبعا بيكون الافضل انك تستخدم ال name based virtual host

تعالى بقى نجرب الطريقتين ، علشان نجربهم دلوقتى احنا محتاجين اننا نحدد ال virtual hosts بتاعتنا ، اه وبالمناسبة فى حاجة كده عايزين نقولها وهى ال default virtual host

نبدأ الاول وبعدين نحكى اى موضوع ال default virtual host ده ، مبدئيا كده خليك فاكر انك لما بتبدأ ال virtual hosts فانت على طول ديما بتكتب فى ملف ال configuration تبعك اللى هو 01-vhost.conf بتكتب ديما اول حرف من كل كلمة capital بالشكل ده

vim 01-vhost.conf

<VirtualHost>

وطبعا زى ما بدأت بكلمة virtualhost برضو هتنهى ملف ال configuration بتاعك بكلمة virtual host ، زى ال Html tags بالظبط

</VirtualHost>

وطبعا فى النص بينهم ابدأ حط ال directives اللى انت عايزها ، بالمناسبة كمان فى عندك كده special directive اسمه

<VirtualHost _default_:80>

وده عبارة عن very special directive ، وده بي serve ال default web site بتاع الاباتشى ، بمعنى ان انت لو عملت enable ليه جمب التاج الاولانى ده اللى هو

<VirtualHost>

فده هيعمل overwrite لل main server configuration ، وخليك فاكر النقطة دى كويس اوى ، ومش كده وبس ، دا فى عندك برضو special directive اسمه **asterisk *** وبالشكل ده هيبقى معناه اى ip

<VirtualHost *:80>

وده برضو هيعمل overwrite لل default server configuration ، فالاتنين واحد سواء كنت هتخليها

default :80

او كنت هتخليها *:80

بعد كده هتبدأ تحدد ال **DocumentROOT** اللى هو طبعا المكان اللى الاباتشى هي serve منه ملفات ال HTML بالشكل ده

<VirtualHost>
DocumentRoot /opt/main/www

</VirtualHost>

وطبعا متنساش برضو فى كلمة DocumentRoot ان اول حرف من كل كلمة بيكون Capital ، بعد كده هتحددله ال logs بالشكل ده

<VirtualHost>
DocumentRoot /opt/main/www
CustomLog "logs/default-vhost.log"
</VirtualHost>

طبعا انت بالشكل ده انت كده كأنك لغيت المسار اللى اسمه

/var/www/html

اللى كان الاباتشى بي serve من ملفات ال `main web site`

وطبعا انت هتضطر انك تعمل directory بالشكل ده زى ما انت حددته فى ملف ال configuration بتاعك

mkdir -p /opt/main/www

وطبعا احنا استخدمنا ال option اللى هو

-p

لان احنا هنعمل directory 2 فى ال /opt

-p ====> parents

تعالى بقى فى المسار ده واعمل ملف ال index.html الرئيسى الخاص بال main web site مثلا بالشكل ده

vim /opt/main/www/index.html

وبعدها بقى اعمل restart لل httpd

systemctl restart httpd

بص خلى بالك انك لو جيت تعمل restart لل httpd بعد ما عملت ملف ال configuration الخاص بال virtual host ، لو الملف فيه اخطاء مش هيعمل restart لل httpd وهيقولك الرسالة دى

[root@server ~]# systemctl start httpd
Job for httpd.service failed because the control process exited with error code. See "systemctl status httpd.service" and "journalctl -xe" for details

طبعا انت لازم تتعود كل مرة تظهرلك فيها الرسالة دى ، تجرى بسرعة تنفذ الامر اللى هو قايلك عليه وهو

journalctl -xe

علشان تشوف الاخطاء اللى منعت ال os من انه يعمل restart لل httpd وتتفاجأ انها اخطاء بسيطة بالشكل ده

Jul 25 11:21:39 server.apache.com httpd[1110]: AH00526: Syntax error on line 1 of /etc/httpd/conf.d/01-vh...onf
<VirtualHost> directive requires additional arguments

يعنى بيقولك ان ملف ال configuration بتاعك فيه syntax error فى السطر رقم 1 ، والسطر اللى بعده بيشرحلك فيه سبب المشكلة وبيقولك اى اللى انت لازم تعمله

المهم بعد كده تيجى تعمل restart لل httpd ، تتفاجأ برضو ان لسه فى مشكلة فى ملف ال configuration بتاعك وتيجى تنفذ الامر

journalctl -xe

هيطلعلك الناتج ده

AH00526: Syntax error on line 3 of /etc/httpd/conf.d/01-vhost.con
Jul 25 11:32:00 server.apache.com httpd[1584]: CustomLog takes two or three arguments, a file name, a custom log

بيقولك برضو ان فى syntax error فى الملف فى السطر التالت ، وبيشرحلك ان ال CustomLog اللى هى ممكن تعتبرها function او مثلا command وبيقولك بقى ان ال CustomLog دى بتقبل 2 arguments او 3

يبقى انت كده هتزود كلمة combined فى سطر ال CustomLog ، علشان تقوله ضملى الكلام ده كله مع بعض

<VirtualHost _default_:80>
DocumentRoot /opt/main/www
CustomLog "logs/default-vhost.log" combined
</VirtualHost>

وبعدها تعمل restart لل httpd هتلاقيها اشتغلت معاك وتعالى بقى روح جرب فى المتصفح ، هتلاقيه بيقولك رسالة ال error دى

Forbidden

You don't have permission to access / on this server.

ليه الرسالة دى ظهرتلك ، لان ببساطة ، تعالى ارجع كده لملف ال configuration الرئيسى بتاع الاباتشى هتلاقى عند ال block directory دى

```
<Directory />
    AllowOverride none
    Require all denied
</Directory>
```

هتلاقيه هنا ان الاباتشى مش مسموح ليه انه يعمل serve من اى مكان تانى غير المكان اللى هو

/var/www/

وبالتالى انت هتروح لملف ال configuration بتاعك وتضيف فى اخره ال block directory دى

<Directory /opt/main/www>

Require all granted

</Directory>

وهوب تعمل restart لل httpd تانى وهتلاقى المشكلة اتحلت معاك ان شاء الله

يبقى انت كده طالما عملت ال default server configuration

فهو كده هيعمل overwrite لل Main Server Configuration

دلوقتى بقى لو حبيت تعمل virtual host جديد ، هيبقى الموضوع برضو بسيط جدا ان شاء الله ، كل اللى عليك هو انك تعمل ملف configuration جديد تانى

مثلا بقى خد نسخة من الملف الاول واعمل واحد تانى جديد

cp 01-vhost.conf 02-vhost.conf

وتعالى بقى افتح الملف التانى ده

vim 02-vhost.conf

وهيكون بالشكل ده

<VirtualHost *:80>

DocumentRoot /data/www.ahmed.com/www

CustomLog "logs/ahmed-vhost.log" combined

</VirtualHost>

<Directory /opt/www.ahmed.com/www>

Require all granted

Allow from all

</Directory>

طبعا متستغربش عادى اسم المجلد ممكن يكون كده

www.ahmed.com

مفيهاش حاجة يعنى وبعدين تيجى تعمل ال dirctory بقى اللى هتحط فيها ملفات ال web site التانى بالامر ده

mkdir -p /data/www.ahmed.com/www

دلوقتى بقى بما انى بستخدم ال name based virtual hosting ، فكده ملف ال configuration التانى ده ناقصه شوية حاجات زى ال **ServerName** وممكن تضيف كمان ال **ServerAlias**

يعنى مثلا الاسم المرادف للموقع بتاعك ، بالشكل ده

<VirtualHost *:80>
ServerName www.ahmed.com
ServerAlias ahmed.com
DocumentRoot /data/www.ahmed.com/www
CustomLog "logs/ahmed-vhost.log" combined
</VirtualHost>
<Directory /data/www.ahmed.com/www>
Require all granted
</Directory>

وبعدها بقى تعمل restart لل httpd ، وتروح بقى على المتصفح وتيجى تجرب ال ip بتاع السيرفر ، هتلاقيه برضو بي serve ال main web site وليس ال web site التانى اللى هو

www.ahmed.com

والحقيقة ان انا هنا عندى مشكلة ، دلوقتى انا عامل للاباتشى انه يستخدم ال name based virtual host ، وعلشان تقدر انك تستخدم ال name based virtual host لازم ال client يحاول انه يعمل connect عن طريق الاسم ، يعنى يكتب فى المتصفح بتاعه www.ahmed.com
بس هنا ال client مش هيقدر انه يعمل resolve للاسم بتاع ال web site ده

حتى لو اتنطط ، والسبب انى لسه معملتش DNS او معملتش Setup لل DNS حتى الان ، والحل هنا مؤقتا انى اهارد كود hard code اسم ال web site ده فى ملف ال hosts عند جهاز ال client

اوباااااااا هنا بقى فى ملحوظة كبيرة فشخ ، وهى ان الاباتشى مش هينفع ي serve كل ال virtual hosts غير من directory واحدة بس ، يعنى بالسلامة كده العك اللى انت عملته فوق ده مينفعش وهو انك تحددله مكان تانى غير ال **/opt**

انه يعمل serve منه زى ما انت عكيت وعملت directory تانية اسمها **/data**

كده انت هترجع تعدل تانى فى ملف ال configuration اللى هو

02-vhost.conf

وتعدل ال DocumentRoot وال allowed directory بالشكل ده

```
<VirtualHost *:80>
ServerName      www.ahmed.com
ServerAlias     ahmed.com
DocumentRoot    /opt/www.ahmed.com/www
CustomLog       "logs/ahmed-vhost.log" combined
</VirtualHost>
<Directory /opt/www.ahmed.com/www>
Require all granted
Allow from all
</Directory>
```

روح بقى على المتصفح وجرب تكتب www.ahmed.com وانت على جهاز ال client هتلاقيه فتح معاك وبكده بقى عندنا سيرفر واحد ومرفوع عليه اكتر من web site عن طريق ال virtual hosts

7-SSL

بص قبل ما نبدأ فى موضوع ال **SSL** لازم تتفرج على كام فيديو كده موجودين فى ال **Playlist** اللى قولنا عليها فوق وده لينك اول فيديو بيشرح ال **GPG**

https://www.youtube.com/watch?v=uAYw84jYPGY&t=0s&list=PLCIJjtzQPZJ_10_h-jzD299qkg_IuoT-5&index=12

وده لينك الفديو التانى لازم برضو تتفرج عليه

https://www.youtube.com/watch?v=UQWANU482qU&t=0s&list=PLCIJjtzQPZJ_10_h-jzD299qkg_IuoT-5&index=13

وده لينك الفديو التالت اللى بيشرح فيه البشمهندس مصطفى حموده موضوع ال **SSH** لازم برضو تتفرج عليه

https://www.youtube.com/watch?v=_mNZZjWHgPo&t=0s&list=PLCIJjtzQPZJ_10_h-jzD299qkg_IuoT-5&index=14

نبدأ بقى فى موضوع ال SSL ، بص يا سيدى سيبك دلوقتى من ال ssl وتعالى نشرح الفكرة بتاع ال Public Key Infrastructure ، او اى اصلا ال Public Key وال Private Key ده ؟

مبدئيا كده انا بيكون عندى يوزر موجود وال user ده بيكون عايز يعمل connect مع مكنة بشكل secure ، دلوقتى بقى الراجل ده هي connect ازاى ؟؟

بص يا سيدى الفكرة كلها قايمة ان المكنة دى هعمل عليها حاجتين بساط جدا هعمل عليها حاجة اسمها ال Public Key وحاجة تانية اسمها ال Private Key

دلوقتى بقى ال Private Key ده من اسمه هيكون عبارة عن secret Key ، انما ال Public Key اديه لاى حد او لاى مستخدم تانى ، لانه مش هيفرق معاك مين اللى هياخده

طيب اى برضو موضوع ال Public Key وال Private Key ده ؟ قالك بص يا سيدى كل Private Key هيكون ليه ال Public Key بتاعه

دلوقتى بقى لو انت عندك داتا ، والداتا دى انت عملتلها encrypt ، يعنى اعتبرها بالظبط زى القفل ، بس القفل ده ليه مفتاحين ، بمعنى انك لو عملت encrypt بمفتاح لازم تعمل Decrypt بالمفتاح التانى

بمعنى اخر انك لو عملت encrypt بال Private Key فانت هتعمل Decrypt بال Public Key والعكس صحيح ، بمعنى اخر لو انت عملت encrypt بال Public Key ، فالشخص الوحيد اللى هيقدر يعمل Decrypt هو الشخص اللى معاه ال Private Key بس **لذلك ممكن تعتبر ان ال Private Key وال Public Key هما عبارة عن قفل بمفتاحين اتنين ، وعمر القفل ده ما هيتفتح غير لما المفتاحين يكونوا موجودين** ، لحد كده تمام

دلوقتى انا قولتلك ان ال Public Key ده ممكن تديه لاى حد فى الدنيا او ممكن يكون مع اى حد ، انما ال Private Key ده هيكون موجود على السيرفر او المكنة بس

خلى بالك برضو ان السيرفر عنده الاتنين ال Private Key وال Public Key ، انما ال Client بيكون عنده ال Public Key بس ، دلوقتى بقى لما السيرفر يحب يبعت داتا لل client هيستخدم طبعا ال Private Key ، واكيد طبعا ال Client لما ياجى يعمل Decrypt هيستخدم ال Public Key

انما دلوقتى ال Client لما ياجى يبعت للسيرفر ، دلوقتى ال Client مش معاه غير ال Public Key فاكيد هيستخدمه وبالتالى السيرفر هيستخدم ال Private Key علشان يفك الداتا اللى ال Client باعتها

كده السيرفر عليه الاتنين Keys ، لما يحب يبعت لحد اى داتا ، فال Public Key بتاع السيرفر هيكون مع الناس كلها وبالتالى هو لما يحب يعمل encrypt هيستخدم ال Private Key بتاعه وبعد كده بقية الناس تفك التشفير ده بال Public Key

هنا بقى المشكلة الحقيقية ان ال Public Key بيكون مع اى حد ، معنى كده ان اى حد معاه ال Public Key هيقدر انه يفك الداتا اللى السيرفر بيبعتها ، وده طبعا سؤال ممكن ياجى فى ذهنك على طول ، بس هنا بقى استنى هقولك على حاجة وهى ان الموضوع اكبر من كده بكتير ، ليه بقى ؟؟؟ لان اصلا ال Client لما ياجى ي connect على السيرفر لازم ي initiate session يعنى لازم بيفتح session معينة ، وال session دى بيكون ليها session key ، يعنى مش مجرد session عادية ، لا ، دى بتكون session encrypted كمان

وطبعا ال Session Encrypted دى بتكون encrypted عن طريق ال Public وال Private Key ، طيب اصلا اصلا ال Session Keys دى ذات نفسها بتيجى منين بقى ؟؟ قالك ان ال session keys دى بتكون عبارة عن random keys وال Client والسيرفر بيتفقوا عليها مع بعض عن طريق algorithm اسمه الديفى هلمن اختصاره **DH**

اى بقى ال DH ده هو كمان ؟ بص الديفى هلمن ده عبارة عن الجورزم بسيط كل وظيفته فى الحياة انه يخلى طرفين ميعرفوش بعض خالص انهم يتكلموا لاول مرة وكل واحد فيهم عنده session key مختلفة وطبعا ال session key دى بيتعملها generate بشكل random ، يعنى كل واحد بيحاول انه يعمل keys خاصة بيه ، وبعد ما كل واحد فيهم سواء من السيرفر او ال client يعملوا ال keys الخاصة بيهم ، كده الاتنين يقدروا يتفقوا بعد كده على session key معينة ومش كده وبس ، بعد كده ال DH ده او الالجورزم ده هيسمحلهم فى المستقبل انه يعمل renew لل Session Key دى زى ما هو محتاج او حسب الحاجة اليه ، معنى كده ان الموضوع مش متساب مفتوح ع البحرى يعنى مش اى حد معاه ال public key يقدر انه يفك وخلاص كده

لا طبعا ، لان ال session اللى بين ال client وبين السيرفر هتكون ديما encrypted وكمان الاتنين هيتفقوا مع بعض على session key معينة وال session key دى هيستخدم الجورزم اسمه ال DH علشان الاتنين برضو يتفقوا على session keys معينة ، تحس ان الموضوع فيه لعبكة

طيب دلوقتى علشان تفهم ال DH ده فى فديو على اليوتيوب بيوريك ازاى الاتنين اللى هما السيرفر وال client بيتفقوا مع بعض ، اكتب Diffie Hellman وفى الفديو ده بيشرح ازاى طرفين ، سواء سيرفر وسيرفر ، او حتى client و client ازاى انهم يكلموا بعض بشكل secure من غير ما ال key اللى بينهم يتعرف

لازم تتفرج على الفديو لانه جميل ده ، وطبعا تتفرج على فديو البشمهندس مصطفى حمودة من اول الدقيقة 10 فى الفديو رقم 72

طيب هنا الموضوع هيكون حسابى اكتر او رياضى اكتر

المهم نرجع بقى لموضوعنا ، وهو ازاى انا ا create ال Private key وال Public Key بتوع السيرفر ، وانا طبعا هكون بطبق الكلام ده على جهاز السيرفر مش عند ال client اوعى تتلغبط ؟

طيب علشان تعمل الكلام ده عند السيرفر ، فى عندك utility بيسطة كده ممكن تسطبها على جهاز السيرفر بالامر التالى

yum search crypto-utils

وبالمناسبة فى tool هنعملها install ، اسمها ال Open SSL ، ودى عبارة عن Framework كاملة هتستخدمها علشان تتعامل مع ال Public Key وال Private Key Infrastructure بالكامل

تعالى بقى سطب ال utility دى

yum install crypto-utils

وكل فكرة ال crypto-utils انها بتسمحلك انك تعمل Public Key و Private Key بكل سهولة

انما بالنسبة لل open ssl فال syntax بتاعها مش بسيط ، لانه فى syntax علشان ت generate ال Private Key و syntax تانى علشان ت generate حاجة اسمها certificate signing request و syntax علشان تعمل حاجة اسمها Public Key يعنى شغلانة كبيرة ، انما ال crypto-utils هتسمحلك انك ت generate ال public key وال private key بشكل مبسط جدا

دلوقتى لو رجعنا بس لموضوعنا، هنلاقى اننا عندنا مشكلة تانية ، دلوقتى احنا خلاص عرفنا ال session keys اللى بين ال client والسيرفر انها هتكون secured ديما وطبعا الاتنين هيتفقوا عليها عن طريق الجورزم اسمه Diffie Hellman ، دلوقتى بقى المشكلة الحقيقة مش فى كده خالص ، المشكلة الحقيقية هنا وهى ان ازاى ال Client ده هي trust السيرفر ، يعنى اى اللى يضمن لل client ان السيرفر ده مش fake وان مفيش حد قاعد يعمل DNS Poisoning بدل ما يروح للموقع الفلانى ده ، يروح لموقع fake ال Man In The Middle هو اللى عامله ، اى بقى اللى يضمن ان السيرفر ده trusted بالنسبالك ؟

بص مفيش حاجة هتضمن كده غير ان ال Public Key اللى عندك وعند السيرفر لازم بقى ال key ده يكون ذات نفسه trusted ، وعلشان ال Public Key ده يكون Trusted بالنسبة لل Client او ال user ، قالك بس انا هجبلك جهة تالتة كده اسمها ال **Certificate Authority** واختصارها هو **CA** ، اى بقى ال certificate authority دى ؟ قالك ان دى عبارة عن جهة وظيفتها انها تأكدلك ان ال Public Key دى مظبوط $100 و Trusted

طب ازاى بقى ؟؟ قالك انا هاخد ال Public Key من السيرفر او السيرفر هيبعت ال Public Key بتاعه لل CA وبعدين ال CA تروح تختم على ال public key ده ، يعنى تحط ال signature بتاعتها على ال Public Key ده وبعدين تبعته للسيرفر تانى وبيكون هنا اسمه certificate

يعنى ال certificate فى الاصل عبارة عن ال Public Key وال signature بتاعت ال CA ، بكل بساطة ال certificate ، ممكن تقول عليها هى ال **Signed Public Key** ، يبقى كده ال Client لما ياجى يعمل connect على السيرفر هيلاقى ان ال Public Key عليه ال signature بتاع ال Certificate Authority ، طيب برضو ال Client هيعرف منين ان ال Certificate Authority دى Valid ولا لأ منين ؟؟ نفس حكاية السجل المدنى

اصلا اصلا ال Certificate Authority انت بتبقى عارف عنها مسبقا ، وبالمناسبة ممكن يكون عندك اكتر من certificate authority بتوثق ال public key ،زى ما فى اكتر من ختم نسر مثلا ختم نسر بتاع السجل المدنى وختم نسر بتاع المحكمة وهكذا ، وبالمناسبة انت ك client هتلاقى معظم ال CA معمول ليهم embeded فى ال browser عندك

طبعا انت مثلا ممكن تفتح جوجل كروم وتروح ل settings وتدور على كلمة cert هتلاقى عندك list كبيرة بال Trusted Authorities وبالتالى اى شهادة جايالك من الناس دى فانت اوتوماتيك بتثق فيهم ، يبقى دلوقتى لو جاتلك اى شهادة مش موثقة من اى CA ، يبقى معناها حاجة من اتنين ، يا اما ان السيرفر اللى بعت الشهادة دى اللى عبارة عن ال public key زائد ال signature وهنا ال signature بيكون fake

يا اما بقى ان السيرفر اللى بعت الشهادة دى عبارة عن سيرفر fake يعنى واحد بيعمل DNS Poisoning وبالتالى انت تبعد عنه ، او يا اما ان ال Public Key دى فعلا مظبوط بس السيرفر لسه موثقش ال Public Key ده من ال CA ، وهنا بقى القرار بيرجعلك يا اما انك تقبل ال Public Key ده ، او يا اما انك ترفضه

هنا بقى احنا اللى هنعمل ال Public Key بنفسنا ، واحنا كمان اللى هنحط ال signature عليه ، هنوثقه يعنى ، طبعا الكلام ده مينفعش يتعمل فى Production Environment لان انت مش معقول هيكون عندك Public سيرفر ، وكل شوية تعذب ال Clients معاك فى انهم كل شوية يقبلوا ال certificates دى

تعالى بقى حالتنا دى نعمل ال Keys بتاعتنا وكمان نضمنها بنفسنا يعنى نتأكد انها تمام ، تعالى بقى على جهاز السيرفر واكتب

genkey

واول ما تضغط انتر ، هتلاقيه بيطلب منك ال server name اللى هو برضو ممكن تقول عليه اسم الموقع بتاعك ، بالشكل ده

genkey www.ahmed.com

اول ما تضغط انتر ، هتلاقيه بيقولك ان لسه فى Packge ناقصة اسمها mod_ssl ، ودى مسؤلة عن انها تسمح للاباتشى انه يعمل enable لل ssl

package mod_ssl is not installed It is required to generate this type of CSRs or certsfor this host

تعالى بقى سطبها

yum install mod_ssl

تعالى بقى نفذ الامر السابق من تانى

genkey www.ahmed.com

هتظهرلك رسالة مضمونها انه بيقولك انه هيعمل private key هيتخزن فى المكان ده

/etc/pki/tls/private/www.ahmed.com.key

وكمان هيعمل certificate هتكون موجودة فى المكان ده

/etc/pki/tls/certs/www.ahmed.com.cert

وبيقولك كمان ان ال certificate اللى هيعملها دى هتكون عبارة عن Self Side Certificate وكمان بيقولك انه بشكل اختيارى Optional يعنى ، انك ممكن تاخد ال certificate دى وتبعتها ل Certificate Authority

دوس بقى next ، وهتلاقيه بيسألك انت عايز ال key size بتاع ال certificate دى حجمه قد اى بالظبط ؟؟ وبالمناسبة ال key size ده هو اللى هيتم استخدامه بعد كده فى عملية ال encryption بتاع ال Session بين ال Client والسيرفر ، طيب دلوقتى ال key ده ليه size ، وكل ما زاد الحجم بتاع ال key ده كل ما ال session كانت secure اكتر

يعنى كل ما عملية ال encryption كانت بتم بشكل اكبر باستخدام size اكبر ، كل ما عملية ال decryption هتاخد وقت اكتر هى كمان ، وبالتالى حاول توازن بين ان ال key بتاعك يكون مش طويل اوى ولا قصير اوى ، طبعا هتلاقيه هو محددلك ال recommended size ، وبرضو فى الاخر خالص ممكن تديله انت ال size اللى انت عايزه بالظبط

احنا هنا هنستخدم ال recommended size وبعدين next وتستنى عليه شوية ، طبعا هو هنا بقى هيحاول انه ي **generate random bits** علشان يعملك ال Public وال Private Key بتوعك

طبعا لو عايزه يعمل generate للل random key بشكل سريع ، يبقى تنشط السيرفر بتاعك عن طريق الكام امر

ls -lhR /

cat /dev/random >> /dev/null

tree /

طيب ال **CSR** هى اختصار ل **Certificate Signing Request**

بيقولك بقى بعد كده انت عايز تبعت ال certificate signing request للل certificate authority ولا لأ ؟ طبعا ال certificate signing request ده عبارة عن ال Public Key بتاعك اللى بيتبعت للل certificate authority علشان تمضيلك عليه ، احنا هنا هنختار No

بعد كده بيقولك انت عايز تعمل encrypt للـ Private Key ذات نفسه ؟ لو انت عملت encrypt ليه ، فانت كل مرة هتستخدمه هيطلب منك username و password وطبعا ده مش عملية Practical ابدا مع الاباتشى ، لان انت كل مرة هتعمل restart للـ service بتاعت الاباتشى هيطلب منك الباسورد اللى انت عملتها دى

دوس بقى next وتعالى بقى فى الصفحة الجاية دى نحط الـ information بتاعت الـ Key بتاعتنا ده

هيطلب منك اسم الدولة ، تكتب حرفين بس ، بالشكل ده

```
|
|        Country Name (ISO 2 letter code) EG_                    |
|      State or Province Name (full name) CAIRO_____________      |
|            Locality Name (e.g. city) NewCairo_____________      |
|        Organization Name (eg, company) AHMED.COM_____________  |
|    Organizational Unit Name (eg, section) IT_____________________ |
|                                                                 |
| Common Name (fully qualified domain name) www.ahmed.com_____________ |
|
```

بالنسبة لـ IT فده اسم السيرفر بتاعك ، اى حاجة يعنى اكتب اى اسم

بس خلاص كده هو خلص ،هيقولك بقى فين ال Private Key بتاعك ، وفين ال certificate

خد بقى مكان ال certificate ده copy

/etc/pki/tls/certs/www.ahmed.com.crt

وتعالى بقى روح لل configuration بتاع ال ssl فى المكان ده

vim /etc/httpd/conf.d/ssl.conf

هتلاقى برضو ملف ال ssl ده بسيط جدا هو كمان ، زى مثلا هتلاقى السطر ده

Listen 443 https

يعنى بي listen على بورت 443 ، وكلمة https دى كلمة optional يعنى ممكن تمسحها ، لانه اصلا بي listen على https او على 443

بعد كده بقى انزل تحت خالص ، لحد ما تدور على السطر ده

SSLCertificateFile /etc/pki/tls/certs/localhost.crt

بيسألك فين ال ssl certificate file بتاعك ، فانت هتحطله مكان ال certificate file بالشكل ده

SSLCertificateFile /etc/pki/tls/certs/www.ahmed.com.crt

وكمان برضو تعالى على السطر ده

SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

وحطله ال private key

SSLCertificateKeyFile /etc/pki/tls/private/www.ahmed.com.key

وبعدين تعمل restart للاباتشى

systemctl restart httpd

طيب دلوقتى الكلام ده اللى احنا عملناه كان لل main server configuration

بعدها بقى لازم تخلى ال firewall يسمح لل https ك connection انه يعدى

firewall-cmd --add-service=https --permanent

firewall-cmd --reload

تعالى بقى فى المتصفح واكتب

https://www.ahmed.com

وهتلاقيه طلعلك تحذير وهو ان ال Certificate authority مش Trusted ، ده معناه برضو ان ال Public Key مش trusted بالنسبة لل browser لانه معمول ليه sign عن طريق CA المتصفح مش واثق فيها اصلا

لو روحت للمتصفح وشوف معلومات ال certificate اللى احنا عملناها هتلاقيها valid لمدة شهر بالظبط تقريبا ، علشان كده احنا محتاجين اننا نعمل renew لل certificate دى بعد شهر

طيب فى ملحوظة هنا وهى اوعى تاخد ال Private Key بتاعك وتوديه لل Certificate Authority لان انت كده بتؤذى نفسك

وبالمناسبة كمان اوعى تستخدم ال bit algorithm key 512 فى عملية التشفير لانه بقى disabled بسبب انه مش secured خالص

طيب دلوقتى بقى بعد ما عملنا ال ssl certificate لل domain اللى اسمه www.ahmed.com ، تعالى بقى افتح ملف ال configuration بتاع ال virtual host ده اللى انت عايز تضيفله ال ssl certificate ، عن طريق الامر ده

vim /etc/httpd/conf.d/01-vhsot.conf

وهتخلى شكل الملف بالمنظر ده

```
<VirtualHost *:80>
ServerName      www.ahmed.com
DocumentRoot    /opt/main/www
CustomLog       "logs/default-vhost.log" combined
</VirtualHost>

<VirtualHost *:443>
ServerName      www.ahmed.com
DocumentRoot    /opt/main/www
CustomLog       "logs/default-vhost.log" combined
</VirtualHost>

<Directory /opt/main/www>
Require all granted
</Directory>
```

يعنى من الاخر انت بس هتعمل copy لل tag اللى هو VirtualHost ،
وتخلى نسخه تحته ، بس بدل ما هو هي Listen على Port 80 ، لا انت هنا
هتخليه ي listen على 443 بورت اللى هو بتاع ال SSL ، ده البورت ال
secure طبعا

كمان انت ممكن تغير مكان ال logs بتاع ال ssl هنا ، وكمان ممكن تقوله انك
عايز تفعل ال **SSLEngine** وكمان لازم تقوله على مكان
ال SSLCertificateFile وبرضو ال SSLCertificateKeyFile ، بالشكل ده

```
<VirtualHost *:80>
ServerName      www.ahmed.com
DocumentRoot    /opt/main/www
CustomLog       "logs/default-vhost.log" combined
</VirtualHost>

<VirtualHost *:443>
ServerName      www.ahmed.com
DocumentRoot    /opt/main/www
CustomLog       "logs/ahmed-vhost-ssl.log" combined
SSLEngine       on
SSLCertificateFile      /etc/pki/tls/certs/www.ahmed.com.crt
SSLCertificateKeyFile  /etc/pki/tls/private/www.ahmed.com.key
</VirtualHost>

<Directory /opt/main/www>
Require all granted
</Directory>
```

خلى بالك ان www.ahmed.com.crt كلمة **crt** بدون حرف ال e علشان متتلغبطش بس

تمام كده وبعدها بقى ، اعمل restart لل httpd ، وبعدين بقى تروح للمتصفح وتجرب

https://www.ahmed.com

هتلاقيه دلوقتى مش بيبص على ال main web site ولكن دلوقتى رجع لحالته وبقى بيبص على المكان اللى انت حددتهوله اللى هو

/opt/main/www

وكده معناه ان ال ssl certificate الخاصة بال Virtual Hosts دى بقت شغالة خلاص

اه بالمناسبة ال Certificate File اللى هو موجود فى المسار ده

/etc/pki/tls/certs/www.ahmed.com.crt

ده عبارة عن ال Public Key بتاعك

كده معناه برضو ان ال virtual host بقى بي serve ال http connection وال https connection

8-Maria DB

الموضوع ده بسيط جدا ومفيهوش كلام كتير

هنتكلم بقى النهارده عن موضوع مهم جدا وهو ال Dynamic Content ، طيب دلوقتى بقى قبل ما نتكلم عن ال dynamic content ، احنا هنتفرع الاول فى حاجة كده هنتكلم عليها وبعدها بقى هنرجع لل dynamic content ، بمعنى اننا مش هينفع ندخل فى ال dynamic content من غير ما تكون عارف ال basics بتاعت ال data base

الاول تعالى بقى نتكلم شوية عن ال Data Bases ، طبعا زى ما انت عارف ان فى اكتر من نوع لل data base ، واشهرهم ال SQL Data Bases والنوع التانى هو ال No SQL Data Bases

طيب دلوقتى بقى ال SQL Data Base عندها مشكلة حقيقية وهى ال Scalibility اى القابلية للتمدد فيها قصور شوية الى حد ما ، طب وليه بقى فى قصور ؟؟ لانه ببساطة طالما انت بتتكلم ان انت عندك جداول يبقى الجدول ده هياخد كام صف وكام عمود ، يعنى اى اقصى عدد من الصفوف ممكن الجدول يستوعبه واى برضو اقصى عدد من الاعمدة

المشكلة التانية برضو وهى فرضا ان ال Data Base بتاعتك Scalable يعنى قابلة للتمدد ، فال Scalibility دى بقى هتوصل لانهى مدى بالظبط ، يعنى مثلا فرضا ان ال DB بتاعتك هتاخد 50 مليون صف ، طب انت دلوقتى لما تيجى تقسم الداتا على اكتر من سيرفر ، هتقسمها ازاى برضو ، وطبعا الموضوع هيكون مزعج جدا بالنسبالك ، وكل ما هتحل خازوق هيطلعلك 10 قصاده حتى لو انت عملت Cluster وقسمت الداتا او حتى عملت Data Base Partitioning ، فانت برضو هتوصل لمرحلة وهى ان ال SQL Data Bases دى معتش نافعة باى حال من الاحوال ، يعنى احنا وصلنا لمرحلة ان مثلا 100 مليون record او حتى 500 مليون ريكورد ، مبقوش كفاية خالص ، وطبعا عصر ال Big Data لما ظهر خلى الموضوع بقى كبير جدا ، وعندك مثال الفيس بوك وامازون مثلا ، فانت عندك حرفيا مئات الملايين من ال records اللى بتطلع كل يوم ، عندك مثلا امازون لو انت عملت اكونت هناك ودخلت بحثت عن اى منتج مثلا وليكن Mac Book وجيت انت مشترتهوش ، فانت البحث بتاعك ده هيسجل تبع الاكونت بتاعك ، وممكن تيجى بعد كام يوم كده تلاقى امازون بتقولك انك كنت عملت بحث عن ماك بوك واحنا عملنا discount عليه

فا لو انت بتتكلم عن ال SQL Data Base ، فا خلاص ال Scalibility بتاعتها معتش بتنفع ، فكان الحل انهم يفكروا فى approach جديد خالص يعنى حل جديد خالص

وال approach ده او المفهوم ده بيتكلم عن المفاهيم كلها هتتغير من A to Z ، وطبعا هما فكروا فى حاجة اسمها ال No SQL Data Base ، وهنا قالك بقى انسى الخازوق بتاع زمان ده وهو ان كل حاجة عبارة عن جداول والجداول دى عبارن عن صفوف واعمدة والهرى ده ، هنا بقى ال data base بتاعتى هتكون عبارة عن شوية records وكل records هتكون متخزنة فى file

طيب دلوقتى انت هتسأل اى بقى الميزة اللى بتقدمها ال No SQL Data Base هقولك انها حلت مشكلة ال Fixed Size اللى كانت عند ال SQL Data Base ، بمعنى ان ال SQL Data Base سواء سجلت فيها او ما سجلتش فهى كده كده خلاص حجزت مساحة

لكن طبعا ما زالت ال SQL Data Base ، ليها دورها فى الخمس سنين الجايين ان شاء الله ، وده ببساطة مش علشان هى احسن من ال No SQL Data Base ولا حاجة ، لا لا لان ببساطة معظم ال softwares اللى اتكتب فى ال 15 سنة اللى فاتت كانت مكتوبة لل SQL Data Base ، انما بقى معظم الحاجات الجديدة اللى بدأت تتكتب بدأت انها تكون compatible مع ال No SQL Data Base

بص من الاخر كده ، شركة oracle لما اشترت شركة Sun Micro-systems حاولت انها تموت ال MySQL لان عندها سياسة الحاجة اللى مش هتجبلك فلوس ، يبقى ملهاش لازمة

وبالتالى ال Developers اللى شاركوا فى كتابة ال MySQL تضايقوا جدا ، وخدوا النسخة ال Open Source بتاعت ال MySQL وعدلوا عليها وطلعوا لينا بحاجة اسمها ال **Maria DB**

وكمان ال Performance بتاع ال Maria DB بقى احسن بكتير من ال mysql ولحسن الحظ فال Maria DB بتكون Compitable جدا مع ال MySQL بمعنى ان لو فى software كان ال Backend بتاعه هو ال mysql ، فانت ممكن تشغله على ال maria db من غير ما تعدل حاجة ، لان هى اصلا عبارة عن mysql فى الاساس

تعالى بقى نسطب ال mariadb

yum install mariadb

دلوقتى بقى لو قولتله

yum install mysql

هتلاقيه بيقولك ان ال

mariadb is already installed

طيب فى حاجة بقى ، لو انت مصمم انك تشتغل mysql ، فانت ممكن تجيب ال Public Repositories ، الاول نفذ

yum repolist

طبعا زى ما نت عارف ممكن تضيف ال epel وال rpm fussion والكلام ده ، وبالمناسبة ال epel هى اختصار ل

Extra Package For Enterprise Linux

بعد كده بقى هنسطب ال **mariadb-server** ، طبعا اللى احنا سطبناه فوق هو ال **mariadb client**

yum search mariadb | less

yum install mariadb-server

فكده انت عندك 2 باكدج للتعامل مع ال Data Base ، واحدة لل client ، وواحدة للسيرفر ، طب اى بقى ال mariadb client ، بص بكل بساطة دى عبارة عن ال Package اللى هتديك ال tool اللى تخليك تتعامل مع الداتا بيز ك client ، يعنى انك تعمل connect على ال data base وت create ال tables وال rows او انك ت create ال user

انما بقى ال mariadb server ، دى عبارة عن ال service ذات نفسها بكل بساطة

تعالى بقى شوف ال status بتاعت ال mariadb

systemctl status mariadb.service

وطبعا بعدها

systemctl enable mariadb

systemctl start mariadb

systemctl status mariadb

الكوميديا بقى فى الموضوع ، وهو ان ال mariadb بتخزن ال data base بتاعتها فى المكان ده

cd /var/lib/mysql/

طيب دلوقتى بقى لو عايز ت connect على الداتا بيز ، فا لو انت هتعمل connect وانت ك root او حتى كاى مستخدم عادى ، هتكتب بس mysql وتبدأ بقى تتعامل مع ال data base بالاوامر اللى انت عارفها

create database Shop character set utf8 collate utf8_general_ci;

طيب دلوقتى احنا قولنا اننا هنقدر نعمل connect على الداتا بيز عن طريق اى يوزر من غير ما الجهاز ما يطلب منا اى باسورد ، وطبعا الموضوع ده مش خالص secured

دلوقتى بقى انت المفروض تعمل secure للداتا بيز بعد ما تعملها install على طول ، عن طريق شوية حاجات كده ، زى مثلا انك تعمل disable لل remote login واى حد يعمل login فا يطلب منه باسورد

الحاجة التانية انهم من ايام ال mysql ، هما عملوا حاجة اسمها

mysql_secure_installation

وده عبارة عن script بسيط علشان ت secure الدنيا من خلاله

انت دلوقتى لو كتب بس فى الترمنال

mysql_

وضغت tab 2 ، هتلاقى جابلك كل شوية scripts جاهزة ومن ضمنها ال

mysql_secure_installation

```
[root@server ~]# mysql_
mysql_convert_table_format  mysql_plugin              mysql_upgrade
mysql_find_rows             mysql_secure_installation mysql_waitpid
mysql_fix_extensions        mysql_setpermission       mysql_zap
mysql_install_db            mysql_tzinfo_to_sql
```

تعالى بقى اكتب فى الترمنال

mysql_secure_installation

واول ما تكتبها هتلاقيه طلعلك رسالة بيسألك فيها عن ال root password بتاع ال mariadb ، طب انت اصلا مكنش فيه باسورد ، يبقى انت هتضغط enter

بعدها بقى هيسألك اذا كنت عايز تحط password لل root ولا لأ

Set root password? [Y/n]

طبعا هتكتب **y** ،وبعدها هتختار الباسورد تبعك الجديدة ، كل ده وانت ك root اوعى تنسى او ممكن وانت ك user تانى بس باضافة كلمة sudo

بعد كده بقى هل عايز تشيل ال anonymous user ، لانهم ممكن يعملوا connect على ال data base

Remove anonymous users? [Y/n]

طبعا هنشيلهم ، يبقى تكتب y

بعد كده هيسألك اذا كنت عايز تعمل disallow لل root انه يعمل remote login على الداتا بيز دى

Disallow root login remotely? [Y/n]

طبعا هتكتب y ، طب ليه اصلا انت عايز توقف الحوار ده ؟ لان ببساطة لو ال root كان بيعمل login من على شبكة تانية مثلا وبيحاول ان يأكسس ال maria db client فا ممكن يكون فى حد تانى قاعد بي sniff ال connection ده ، وطبعا لو حد بي sniff يبقى هيشوف الباسورد بتاع الرووت بتاع ال data base

طبعا انت كده عندك ال root باسورد بتاع ال OS ذات نفسه ، وكمان عندك ال root password بتاع ال data base ، اللى هو الباسورد بتاع ال administrator بتاع ال data base ذات نفسها

بعد كده بقى اى حاجة تجيلك اكتب y

تعالى بقى اكتب فى الترمنال mysql ، هتلاقيه بيقولك access denied ، يبقى انت هتكتب

mysql -p

وبعدها بقى هتكتب الباسورد بتاعك بتاع ال data base ، والكلام ده بقى مع اى user تانى ، او بالشكل ده

mysql -u root -pahmed

وبالمناسبة الباسورد لازم تكون لازقة فى حرف ال p ، وطبعا الشكل بتاع انك تكتب الباسورد بالشكل ده غير recommended خالص ، علشان لو فيه واحد بيشوف ال history بتاعتك فانت كده لبست نفسك فى الحيط

بالمناسبة لو انت عندك table كبير فانت ممكن وانت بتعرضه بدل ما تصغر الخط فى الترمنال زى ما كنت بتعمل زمان لا دلوقتى انت ممكن تعرضه بالشكل ده

select * from user \G;

وهتظهرلك بالشكل ده

```
MariaDB [mysql]> select * from user \G;
*************************** 1. row ***************************
                Host: localhost
                User: root
            Password: *0A2AE3C3C1A250E03BCCFC2E2BB03F310F635312
         Select_priv: Y
         Insert_priv: Y
         Update_priv: Y
         Delete_priv: Y
         Create_priv: Y
           Drop_priv: Y
         Reload_priv: Y
       Shutdown_priv: Y
        Process_priv: Y
           File_priv: Y
```

Grant_priv: Y
References_priv: Y
Index_priv: Y
Alter_priv: Y
Show_db_priv: Y
Super_priv: Y
Create_tmp_table_priv: Y
Lock_tables_priv: Y
Execute_priv: Y
Repl_slave_priv: Y
Repl_client_priv: Y
Create_view_priv: Y
Show_view_priv: Y
Create_routine_priv: Y
Alter_routine_priv: Y
Create_user_priv: Y
Event_priv: Y
Trigger_priv: Y
Create_tablespace_priv: Y
ssl_type:
ssl_cipher:
x509_issuer:
x509_subject:
max_questions: 0
max_updates: 0
max_connections: 0
max_user_connections: 0
plugin:
authentication_string:

طبعا هتكون هنا احسن وافضل من ناحية القراءة

بالمناسبة انت ممكن بدل ما تستخدم ال script اللى هو

mysql_secure_installation

انت ممكن تعمل الكلام ده كله manually بايدك ، لكن ده هيعذبك حرفيا

طبعا انت هتروح ت select الداتا بيز اللى هى mysql وتغير بقى الباسورد بتاعت ال root وغيره بقى

بالنسبة بقى لل information schema وال performanace Schema دول عبارة عن داتا بيز بتت create بشكل automatic لما تر ال run data base service

دلوقتى بقى لو عندك data base user اسمه ahmed مثلا ، وانت عايز تديله صلاحيات معينة على داتا بيز معينة او جدول معين ، فده بيتم عن طريق الامر ده

```
grant delete,update,insert on dbname.tablename to dbusername;
```

زى كده بالظبط

```
MariaDB [(none)]> grant all on shop.* to 'ahmed'@'localhost' identified by '12345';
```

طبعا متنساش ان الحاجات اللى هى variables تحطها بين single quotes وطبعا ال identifed by بعدها تكتب الباسورد بتاعت ال data base user اللى اسمه ahmed ده

ولو عايز تخليه يعمل login بشكل remotely فانت طبعا هتغير ال local host وتخلى بدالها ال ip بتاع الجهاز

وبالمناسبة طبعا ahmed ده هو Data Base User وليس System User ، خلى بالك كويس من النقطة دى ، يعنى الراجل ده ملوش علاقة بالسيستم نهائى ، يعنى ميقدرش انه يعمل login على الجهاز بتاعك ، يبقى اذا ال data base users ملهمش علاقة بال system users

دلوقتى بقى وانت مختار ال data base اللى اسمها mysql ، شوف بقى جدول ال user وتأكد ان ال user اللى اسمه ahmed ده اتضاف عن طريق طبعا الامر ده

```
MariaDB [mysql]> select * from user \G;
```

هتلاقى فى row بالشكل ده فى تفاصيل ال user اللى انت ضفته وعملتله باسورد بالشكل ده

**************************** 7. row ****************************

Host: localhost

User: ahmed

Password: *00A51F3F48415C7D4E8908980D443C29C69B60C9

Select_priv: N

Insert_priv: N

Update_priv: N

Delete_priv: N

Create_priv: N

Drop_priv: N

Reload_priv: N

Shutdown_priv: N

Process_priv: N

File_priv: N

Grant_priv: N

References_priv: N

Index_priv: N

Alter_priv: N

Show_db_priv: N

Super_priv: N

Create_tmp_table_priv: N

Lock_tables_priv: N

Execute_priv: N

Repl_slave_priv: N

Repl_client_priv: N

Create_view_priv: N
Show_view_priv: N
Create_routine_priv: N
Alter_routine_priv: N
Create_user_priv: N
Event_priv: N
Trigger_priv: N
Create_tablespace_priv: N
ssl_type:
ssl_cipher:
x509_issuer:
x509_subject:
max_questions: 0
max_updates: 0
max_connections: 0
max_user_connections: 0
plugin:
authentication_string:

ممكن برضو تعمل select على كل حاجة من الجدول اللى اسمه db

select * from db \G;

علشان تعرف اى الصلاحيات اللى اليوزر اللى اسمه ahmed ده واخدها وبرضو ممكن تلاقى تضاد فى الصلاحيات لما تنفذ

select * from user \G;

دلوقتى بقى بعد ما انت عملت user او حذفت user من ال data base ، كل ده بقى ملوش لازمة من غير ما تقول لل DBMS
لل Data Base Management System انه يعمل reload للصلاحيات كلها مرة تانية والصلاحيات دى بقى بيتعملها reload من الجدول اللى اسمه user اللى موجود فى الداتا بيز اللى اسمها mysql ، وبالمناسبة الصلاحيات دى بيتعملها reload لما السيرفر او ال OS ذات نفسه ياجى يقوم او يشتغل ، او انت ممكن تجبر السيرفر وتقوله انه يعمل reload للصلاحيات دى بالامر التالى

MariaDB [(none)]> flush privileges;

تعالى بقى وانت يوزر مختلف فى الترمنال بدون ال root ، جرب تعمل connect على الداتا بيز باليوزر الجديد اللى هو ahmed

[vodafone@server ~]$ mysql -u ahmed -p

هتلاقيه فتح معاك ، وهيكون ليه صلاحيات على ال data base اللى انت حددتهاله لكن طبعا الوحيد اللى ليه صلاحيات على اى حاجة هو ال root user بتاع الداتا بيز ذات نفسها

دلوقتى بقى لو عايز تاخد backup من الداتا بيز بتاعتك ، فانت عندك tool اسمها **mysqldump** وطبعا مش عايز اقولك ان جى معاها كمية options كتيرة جدا

وال backup بيتم بالشكل ده، انت هتحدد اسم ال user وبعدها اسم الداتا بيز اللى انت عايز تاخد منها backup

mysqldump -u root Shop -p > shop.sql

وبالمناسبة ال extension اللى هو .sql ده ملوش اى 30 لازمة ، ده ليك انت بس علشان تعرف ان ده sql file ، وبعد ما خدت ال dump بتاعك ممكن بقى تشوف الملف عن طريق ال vim او عن طريق ال less

less shop.sql

طيب افرض برضو انك حبيت تعمل restore لل data base اللى انت خدتها دى بالشكل ده ، كل الحوار انك هتغير ال redirection

mysql -u ahmed Shop -p < Shop.sql

طب لو فيه اصلا جداول موجودة فهو هيعملها drop على حسب برضو ال statements بتاعت الداتا بيز اللى انت عاملها ، بمعنى اي ؟
دلوقتى انت عملت data base اسمها shop وجيت عملت جدول فيها بالشكل ده

create table if not exits

او انك عملت

drop table if exits

دلوقتى بقى لما تيجى تعملها restore ، فا لو فيه جمل زى ال drop فهو هيطبقها ، فانت خد بالك

وكده موضوع ال DB انتهى والحمد لله

نرجع بقى لموضوع ال Dynamic Content بتاعتنا ، واحنا هنا فى الفديو رقم 74

طيب من الاخر كده كل الحوار ان زمان كانت صفحات الويب عبارة عن Static Pages ، بمعنى انا مثلا عندى موقع اخبار ، فانا هروح اعمل صفحات HTML كتيرة لكذا خبر وهكذا

وده مكنش موضوع عملى خالص ، وبالتالى دلوقتى كان لابد من ما يسمى بال Dynamic Content ، يعنى يكون عندى داتا بيز واروح اجيب منها الاخبار وطبعا الحاجات اللى أدت لتطور الكلام ده كله ال **CMS** اللى هى اختصار ل **Content Management Systems**

اللى هى من الاخر كده نظم ادارة المحتوى زى ال **wordpress** ، من الاخر برضو الفديو ده بيتكلم عن ال word press اللى هى زى المنتديات كده وغيرها بقى وطبعا اشهر ال CMS زى ما انت عارف هو ال **wordpress** و **Joomla**

تعالى كده عل السريع ننزل ال wordpress عندنا على جهاز السيرفر

wget https://wordpress.org/latest.tar.gz

tar xvfz latest.tar.gz

وبعدين روح انقله بقى فى المسار مثلا بتاع ال virtual host اللى كان بيمثل ال main web site بتاعك

وبعدين هنسطب ال php وال php-mysql

yum install php php-mysql

ومتنساش

sudo firewall-cmd --permanent --zone=public --add-service=http
sudo firewall-cmd --permanent --zone=public --add-service=https
sudo firewall-cmd --reload

اه بالمناسبة انت بعد ما سطبت ال php هتلاقى عندك ملف configuration جديد اتعمل فى المسار ده

vim /etc/httpd/conf.d/php.conf

طبعا فى الملف ده بيقولك ان ال directory index بتاعك هو index.php

طيب بالمناسبة اسم الاباتشى ك user على centos و redhat اسمه apache ،
يبقى انت هتغير ال permissions بتاع ال directory اللى اسمها wordpress
وتخليها مملوكة عن طريق الاباتشى

chown -R apache:apache /opt/main/www/wordpress

والباقى كله ما هو الا عملية تسطيب لل wordpress ليس الا

اه بالمناسبة ال wordpress هيحتاج منك data base user وليكن اسمه
wordpressuser ، فانت هتفتح ال mysql ، وتعمل اليوزر بالشكل ده وتديله كل
الصلاحيات وتعمل reload للصلاحيات دى

grant all on wordpress.* to 'wordpressuser'@'localhost' identified by 'password';

flush privileges;

وبعدين خلى بالك من الملف ده علشان اسمه فيه example وانت لازم تحذف
كلمة sample دى

cp wp-config-sample.php wp-config.php

وخد بالك من السطر ده

-rw-r--r--. 1 root   root   2.8K Jul 29 12:56 wp-config.php

chown -R apache:apache wp-config.php

وبعدها بقى تعدل فى ملف ال configuration بتاع الوررد برس وتضيف اسم ال data base وال username وهكذا بقى بالشكل ده

vim wp-config.php

وتعدل السطور دى

```
/** The name of the database for WordPress */
define('DB_NAME', 'wordpressdb');

/** MySQL database username */
define('DB_USER', 'wpuser');

/** MySQL database password */
define('DB_PASSWORD', 'wppassword');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

وبعدها بقى تعمل restart لل httpd ، وتروح بقى للمتصفح هتلاقى ال wordpress فتح معاك

طبعا اى حاجة انت هتعملها فى ال wordpress ، هتلاقيها تتخزن فى ال data base بتاعت ال wordpress ، لو عايز تشوفها يبقى تروح على ال

mysql -u root -p

اخر ملحوظة وهى ان ال php جى معاها modules كتيرة على حسب ما انت عايز

yum search php | less

9-Access Restrictions

اخر فديو فى الاباتشى ، بص هو اصلا مش هينفع اننانخلص الاباتشى ، او مش هينفع اننا نقول اننا خلصنا الاباتشى ، لان الاباتشى مواضيعه كتيرة

طبعا زى ما قولنا فى السابق ان ملف ال configuration بتاع الاباتشى متقسم ل 3 اجزاء ، الاول وهو ال Global Configuration ، والتانى وهو ال Main Configuration والتالت وهو ال Virtual Host Configuration ، وقولنا كمان ان ملف ال configuration الاساسى بتاع الاباتشى مش بيحطوا فيه كل ال configuration ، وانما بينادوا على بقية ال configuration من خلال include statment

وطبعا اتكلمنا كمان عن ال SSL ، كده بقى فاضلنا شوية حاجات كده علشان نقول اننا خلصنا ال basics بتاعت الاباتشى زى اننا ازاى نعمل secure ل directories معينة بحيث ان اى حد حب انه يأكسسها ، تطلب منه username و password

دلوقتى بقى ، فرضنا ان انت عندك web application مكتوب ، وال web application ده مش بيسمحلك انك تدخل username و password علشان تعمل authenticate

فانت بقى ساعتها هتضطر انك ت secure ال apache content بحيث ان اى حد يطلبه لازم يدخل username و password ، فده هيكون ال Lab الرئيسى بتاعنا دلوقتى

تعالى نجرب اننا ن secure الملفات بتاعت ال virtual hosts اللى احنا عملناها

vim /etc/httpd/conf.d/02-vhost.conf

طبعا دلوقتى انا عندى الاباتشى مسموح ليه انه يقرأ ال directory دى من ال File System

<Directory /opt/www.ahmed.com/www>
Require all granted
Allow from all
</Directory>

دلوقتى بقى قبل ما اعمل اى حاجة ، تعالى نعمل directory فى المسار بتاع ال virtual host ده

mkdir /opt/www.ahmed.com/www/secured-dir/

وتعالى نحطها جواها ملف برضو

vim /opt/www.ahmed.com/www/secured-dir/test.html

وروح بقى كده جرب فى المتصفح انك تكتب

https://www.ahmed.com/secured-dir/test.html

هتلاقيه طبعا عرضلك المحتوى بتاع الملف اللى هو test.html

دلوقتى بقى احنا عايزين نعمل secure على ال directory دى ، بحيث ان مفيش حد يقدر انه يدخلها وخلاص

ارجع بقى تانى لملف ال configuration بتاع ال virtual host

vim /etc/httpd/conf.d/02-vhost.conf

دلوقتى بقى ال authentication type ، الاباتشى بي support اكتر من طريقة انه يعمل authenticate ومنها حاجة اسمها ال basic authentication ، وفى طريقة ال basic authentication بيطلب منك username وباسورد وي authenticate منك على طول ، والحاجة التانية انه ممكن يعمل authenticate من ال LDAP

يعنى مثلا لو عندك ldap server وال users موجودين فيه طبعا يعنى مثلا بيكون عندك active directory وعايز تخلى الاباتشى انه يطلب ال usernames وال Passwords من ال active directory او من ال IPA فا طبعا ممكن تطلبها عن طريق ال authentication ، وكمان ممكن تطلب kerberos authentication بمعنى انت مثلا لو عندك Kerberos Server وعايز الناس يعملوا authenticate عن طريق ال Kerberos ، وطبعا هنا بقى لو بتتكلم على Tickets من غير username وباسورد ، يعنى لو الراجل ده معاه ticket فانت هتسمحله ولو مش معاه فاكيد مش هنسمحله

احنا هنا بقى كجزء من ال configuration بتاعتنا ، فااحنا هنستخدم ال basic authentication اللى هما ال username وال password الموجودين عندك Locally على الجهاز وطبعا هما موجودين فى ملف خاص بالاباتشى والمفروض اننا هن authenticate بيهم عن طريقهم

تعالى بقى نعمل authenticate عن طريق ال basic authentication ده ، بما اننا فاتحين دلوقتى ملف ال configuration بتاع ال virtual host ،فا احنا هنضيف الكلام ده

اول حاجة نوع ال authentication وهيكون طبعا Basic ، وبعد كده ال Message اللى هتطلع لل user اللى هى ال AutheName ، بعد كده المكان اللى هيكون

فيه معلومات ال authentication ده ، والحاجة الاخيرة خالص وهى انى هطلب منه حاجة required ، يعنى لازم ال user اللى يجيلك يكون valid

الناتج هيكون بالشكل ده

```
<Directory /opt/www.ahmed.com/www>
Require all granted
Allow from all
AuthType Basic
AuthName "Please Provide Username and Password to Proceed...."
AuthUserFile /etc/httpd/conf/htpasswd
require valid-user
</Directory>
```

بعد كده هتعمل طبعا الملف بتاع اللى فيه ال usernames والباسورد ، بس خلى بالك هنا ، الملف ده انت هتعمله بنفس نمط الملف بتاع

/etc/passwd

بمعنى ان انت عندك اصلا utility هى اللى هتعملك اليوزر نيم وجمبه الباسورد بتاعه هيكون متشفر ، وال utility دى اسمها htpasswd ، بالشكل ده

htpasswd -c /etc/httpd/conf/htpasswd ahmed

طبعا ال user اللى اسمه ahmed ، مش لازم يكون موجود بالفعل ضمن ال system users

-c =====> create

خلى بالك ان اسم الملف بيكون htpasswd او htpasword

المهم ، دلوقتى بقى لو انت عايز تكون more specific اكتر ، فانت ممكن تعمل ال secured directory فى جزء لوحدها فى ملف ال configuration بتاع ال virtual host بالشكل ده

```
<directory /opt/www.ahmed.com/www>
Require all granted
Allow from all
</Directory>
```

```
<Directory /opt/www.ahmed.com/www/secured-dir>
Require all granted
Allow from all
AuthType Basic
AuthName "Please Provide Username and Password to Proceed...."
AuthUserFile /etc/httpd/conf/htpasswd
require valid-user
</Directory>
```

كده انت خليت directory عادية ، و directory تانية خالص هى ال secured وبعدين بقى اعمل restart للاباتشى وروح بقى جرب فى المتصفح كده

https://www.ahmed.com/secured-dir/test.html

وهتتفاجأ انه مطلبش منك لا يوزر نيم ولا باسورد ، طبعا هنا انت لازم تبص على ال logs بتاعت الاباتشى ديمافى حالة الاخطاء اللى زى دى

tailf /var/log/httpd/ahmed-vhost-ssl.conf

لان انت هنا كنت عامل ملفين لل logs واحد لل http وواحد لل https ،وبما انك فى المتصفح بتكتب https ، يبى انت هتشوف ال logs بتاعت ال https

طيب نرجع بقى لموضوعنا ، دلوقتى بقى خلينا فاكرين اننا عندنا طريقتين علشان نعمل secured directory ، الاولى وهى انك تحط ال Parameters فى ملف ال configuration بتاع ال virtual host ذات نفسه مثلا ، والطريقة التانية انك تحط نفس ال Parameters دى فى ملف مخفى فى ال directory اللى انت عايز تخليها secured وتسمى الملف بالشكل ده

.htaccess

وتحط جواه ال Parameters بالشكل ده

```
AuthType Basic
AuthName "Please Provide Username and Password to Proceed...."
AuthUserFile /etc/httpd/conf/htpasswd
require valid-user
```

ملحوظة مهمة جدا

بص يا سيدى كل الفكرة انه فى المتصفح مكنش بيطلب منك username ولا password ، بسبب انك جيت على ال secured directory اللى انت عايز تحطلها وقولتله انها Require all granted وكمان قولتله Allow from all ، وده طبعا غلط جدا جدا ، يبقى انت كده هتمسح السطرين دول ، وتخلى شكل ملف ال configuration بتاع ال virtual host بالشكل ده

```
<Directory /opt/www.ahmed.com/www>
Require all granted
Allow from all
</Directory>
```

<Directory /opt/www.ahmed.com/www/secured-dir/>

AuthType Basic

AuthName "Please Provide Username and Password to Proceed...."

AuthUserFile /etc/httpd/conf/htpasswd

Require valid-user

</Directory>

وبعدها بقى تعمل restart لل httpd ، وتروح بقى تجرب فى المتصفح بعد ما تسمح الكاش بتاع المتصفح ، هتلاقيه بيطلب منك username و password اشطاااااات لحد هنا

طبعا الموضوع ملوش علاقة بال **owner** فى بعض الحالات ، يعنى مثلا ال **secured-dir** عادى جدا انها تكون مملوكة لل **root user**

drwxr-xr-x. 2 root root 23 Jul 30 12:24 /opt/www.ahmed.com/www/secured-dir/

فى بعض الحالات بس ، هتحتاج انك تغير ال owner وتخليه ال apache ، يعنى تخلى الاباتشى هو اللى يمسك ال directory دى

كده حوار الملف بتاع ال .htaccess دى ملوش اى تلاتين لازمة دلوقتى ، الا لو انت هتشيل ال parameters اللى موجودة فى ملف ال configuration بتاع الاباتشى

طيب برضو عايزين نعرف اى حوار الملف ده اللى هو ال .htaccess ؟ بص يا سيدى انت لو رجعت لملف ال configuration الرئيسى بتاع الاباتشى ، هتلاقى عندك فى Special Directive كده ، بالشكل ده

```
# The following lines prevent .htaccess and .htpasswd files
from being
# viewed by Web clients.
#
<Files ".ht*">
    Require all denied
</Files>
```

هتلاقيه بيقولك ان اى ملف بيبدأ ب **ht*** ، فالملف ده denied ، بمعنى ان الملف ده مفيش اى user هيقدر انه يطلبه منك ، بمعنى انك لو حاولت تقرأ الملف ده فى المتصفح فالاباتشى هيعملك deny انك تقرئه

كمان متنساش ملف ال log بتاع الاباتشى ، اللى هو ال error_log ، فى الملف ده هتلاقي فيه انك عملت authentication علشان تشوف ال content بتاع ال secured-dir

طب وانا هستفيد من ال logs دى اى ، بص يا سيدى ، قدام شوية هندرس ال security ، وهتتعلم ان شاء الله ان لو واحد حاول يعمل login خمس مرات وفشل ، فانت تروح رازعه block عن طريق ال ip بتاعه

الحاجة اللى بعد كده ، وهو لو انت عندك web application شغال على الاباتشى ده ، وانت عايز تعمل secure لل web application ده ، فانت عندك Package اسمها

yum install mod_security

وال mod_security دى هتسمحلك انك ت secure الاباتشى بتاعك

تعالى بقى لو عايز تعرف كل الملفات اللى نزلت مع ال Package دى ، سواء ملف ال configuration او غيره ، عن طريق الامر

[root@server ~]# rpm -ql mod_security
/etc/httpd/conf.d/mod_security.conf
/etc/httpd/conf.modules.d/10-mod_security.conf
/etc/httpd/modsecurity.d
/etc/httpd/modsecurity.d/activated_rules
/usr/lib64/httpd/modules/mod_security2.so
/usr/share/doc/mod_security-2.9.2
/usr/share/doc/mod_security-2.9.2/CHANGES
/usr/share/doc/mod_security-2.9.2/LICENSE
/usr/share/doc/mod_security-2.9.2/NOTICE
/usr/share/doc/mod_security-2.9.2/README.TXT
/var/lib/mod_security

وتعالى بقى افتح ملف ال configuration بتاع ال Package دى

vim /etc/httpd/conf.d/mod_security.conf

وبالمناسبة انت ممكن تعتبر ال mod_security ده هو عبارة عن web application firewall ، بيحاول انه يبص على ال request اللى جى من ال user ، يعنى مثلا ال firewall ده بيحاول يبص على انهى url ال user بيبص عليه بالظبط

بمعنى افرض دلوقتى ان ال user طلب url معين من السيرفر بتاعك ،اى اللى يضمنلك ان ال url ده مفيش فيه اى خازوق ، يعنى مثلا مفيش فيه SQL Injetion ولا XSS

دلوقتى بقى لو انت اعتمدت على ال firewalld او ال iptables ، انسى مش هيحموك ، لان انت محتاج Level تانى من ال Protection ، انت دلوقتى محتاج level تانى غير الطريقة العادية

وبالتالى انت هتبدأ تت Check ال url اللى الراجل بيطلبه ، يعنى مثلا لو ال url ده بيطابق اوبي match ل Pattern معينة ، يبقى تعمله Allow انه يتطلب

من الاخر كده البشمهندس مصطفى شرح حاجات بسيطة من ال SQL Inection وال XSS ، ودى فايدة ال mod security

يعنى انت هتروح على جوجل وتكتب modsecurity rules ، دلوقتى بقى ال rules دى بقى في منها نوعين ، اول نوع وهو ال free rules ، وفى منها ال Commerial rules

او هتلاقيها على ال GitHub ، او ممكن تكتب فى جوجل mod security xss example ، وبالمناسبة الحوار كله ، لازم انك تدرس web application penetration testing علشان تفهم الكلام ده

طيب فى حاجة كمان وهى انك مش معنى انك نزلت ال rules ، يبقى مش هتلاقي اخطاء ، لان انت مثلا ممكن يكون عندك web application معين بيطلب حاجات معينة ، زى مثلا ان يكون عندك واحدة من ال rules دى تكون turned off ، وخليك فاكر ان ال rules دى لما بتتكتب ، بتتكت بشكل Generic انها تشتغل على اى system

هتلاقى كمان ال activated rules فى المسار ده

cd /etc/httpd/modsecurity.d/activated_rules/

كمان متنساش ان كل rules بتكون compatible مع نسخة معينة

yum install mod_security_crs

لحد هنا وكده احنا خلصنا اغلب المواضيع ال **Basics** الخاصة بالاباتشى

10-DNS

هنتكلم النهارده عن ال DNS ، وده يعتبر من اكبر المواضيع اللى انت هتدرسها ومن المواضيع اللى فيها كلام كتير جدا ، طبعا ال DNS هو واحد من اهم ال Services المهمة بالنسبالك ك system admin مع ال NTP

لان ديما كده ال Infrastructure بتاعت اى شبكة بتكون مرتبطة ب 3 حاجات ال DNS وال Mail Services وال NTP ، واعتبر ان دول هما ال infrastructure بتاعت الشبكة واهمهم بقى واكتر واحدة او اكتر services فيهم بتكون critical هى ال DNS لان من غيرها مفيش حاجة هتشتغل ، يعنى مثلا عادى لو معندكش NTP لان انت ممكن تستخدم Public NTP Server والدنيا هتبقى تمام عندك ، وكذلك الامر برضو بالنسبة لل Mail Server ، هتلاقى شركات ومؤسسات شغالة من غير Mail Server ، لانهم ممكن يكونوا شاريين Public E-Mail Service زى انهم ياخدوا حاجة من جوجل مثلا او انها تكون hosted على النت ، لكن مينفعش يكون فى شركة حتى لو صغيرة جدا انها ميكونش عندها DNS

وبما ان ال DNS هو موضوع كبير ، فاحنا هنحاول نقسمه لاجزاء ، يعنى مثلا لوجيت بصيت على ال Classifications او المواضيع اللى هنتكلم عنها ، ف احنا هنتكلم عن حاجة اسمها ال Forward Lookup وال Reverse Lookup ، وبعد كده هنتكلم على ال Master DNS وال Slave DNS ، الكلام ده كله نظرى ، بعدها بقى ان شاء الله هنخش فى ال Implementation

بعدين هنخش نتكلم عن ال Resource Records الموجودة ،ولو فى وقت كمان ممكن نتكلم عن ال DNS Sec ، وازاى انت ممكن تستخدم ال DNS علشان ت secure ال records بتاعتك

الحاجة التانية وهى ال Integration ، ازاى انك تعمل DNS Forwarding ، او ازاى انك ت integrate ال DNS ده مع حاجة زى ال Microsoft DNS ، وبالتالى هيكون عندنا مواضيع كتيرة جدا فى ال DNS ، فاحنا دلوقتى هنحاول نتكلم على ال DNS Forward Lookup وال Reverse Lookup وهكذا بقى ،

اه بالمناسبة من خلال ال DNS هناخد 2 services الاولى اسمها **unbound** والتانية اسمها **bind** ، ال service اللى هى bind هتكون هى الرئيسية بتاعتك ده الطبيعى بتاعك لو انت شغال فى اى مكان هتلاقيه شغال bind

وبالمناسبة كل ال Commercial Solutions معتمدة على bind ، عندك مثلا لو بصيت لحاجة من الحاجات اللى بتجيب فلوس كتيرة زى Info Blox ودى Completely Based على bind ابقى خش اقرأ عنها https://www.infoblox.com

الحاجة التانية وهى ال unbound ودى بتستخدم ك cashing name server وبرضو هنحاول اننا نتعلم ازاى نستخدم ال bind ك cashing only name server ، كمان فى موضوع مهم جدا وهو ال DNS Views وده من اهم المواضيع بالنسبالك اللى ممكن تستخدمها ، لو عندك مثلا شركة وفى نوع من ال customers بيأكسسوا الشبكة دى ، اعتبر مثلا ان انت عندك guests وهما بيحاولوا يخشوا الشركة دى فانت عايز توفرلهم Internet Access ، وبالتالى انت هتحاول تحمى ال records بتاعتك او ال resource بتاعتك من ان مثلا الشبكة الداخلية اللى عندك الناس اللى بيتصلوا بيها يشوفوا حاجات معينة ، وال guests اللى جايين ليك هيستخدموا نفس ال DNS بس هيشوفوا حاجات تانية ، فهنحاول اننا ن Implement ال DNS Views عندنا واحنا شغاليين

طيب فى حاجة عايز اقولك عليها وهى ان كل ال services اللى موجودة عندنا بتكون بشكل ما مربوطة او tightly integrated مع ال selinux ، فاحنا مؤقتا كده هنعمل disable لل selinux علشان ميحصلناش مشاكل ، لحد ما نوصل لل selinux وهى هتكون بعد ال Mail Server

يلا بقى نبدأ ، بسم الله

بداية كده اى هى معلوماتك عن ال DNS ؟ بص يا سيدى اى resource بتطلبه الطبيعى انك بتطلبه عن طريق ال ip ، يعنى مثلا فى البداية خالص لما الانترنت اتعمل مكنش فيه حاجة اسمها DNS اتعمل اصلا ، كل اللى اتعمل هى ال IP Addresses اللى احنا شغاليين بيها ، ولما اتعملت ال ip addresses كان لازم علشان تأكسس اى جهاز بيكون عن طريق ال ip بتاع الجهاز ده ، وعلشان تأكسس كل ال web sites او كل الاجهزة دى كلها ، فالموضوع كبر منهم خالص
فعلشان يحلوا المشكلة دى ، بدل ما انت كل جهاز علشان تروحله او تحاول تستخدمه لازم تكتب ال IP بتاعه وطبعا الموضوع ده مزعج فى حد ذاته ، فالناس فكروا وقالوا اننا هنبدأ نحط ال ip addresses بالاسماء بتاعتهم فى **/etc/hosts**

رغم ان الحل ده يعتبر نوعا ما كويس ، لكن احنا عندنا مشكلتين دلوقتى ، الاولى وهى حجم الملف ده بقى قد اى يعنى ال size بتاع الملف ده هيكون قد اى

والحاجة التانية وهى ان كل اللى انا بعمله ده بيكون Locally ، وبالتالى احنا عندنا مشكلة كبيرة جدا هنا وهى ان حجم الملف هيكبر اوى وبالتالى عمرك انت ك user ما هتقدر انك ت maintain ملف بالشكل ده ، ليه بقى ؟

لان تخيل ان انت عندك سيرفر وصاحب السيرفر ده نقله من ISP ل ISP تانى ، يعنى مثلا تخيل انت كده مثلا فى مصر وكان صاحب السيرفر ده واخد نت من TeData وهوب راح مغير وصلة النت بتاعته وراح لفودافون مثلا او اتصالات او حتى Link ، وراحت شركة Link ادت ليه IP Addresses جديدة خالص

فا هو كده مضطر انه هيروح لنفس الملف ويشوف الاسماء القديمة اللى كانت متوصلة بالسيرفرات القديمة ويغيرها ويحط ال IP Addresses الجديدة ده كده رقم واحد
الحاجة التانية وهى ان انت لو عندك الف مستخدم ، فالالف دول برضو هيضطروا انهم يعملوا نفس الحوار برضو ، وبالتالى الموضوع مزعج جدا

فعلشان يحلوا المشكلة دى ، قالك بس ، من هنا بدأت الايانا او اللى هى ال **IANA** اختصار ل **Internet Assigned Numbers Authority** قالت هو احنا ليه منعملش Organized way علشان نتحكم فى الاسماء دى كلها ، بحيث اننا منعذبش الناس ونخلى الدنيا سهلة ، فا بدأوا انهم يفكروا فى hierarchy system والسيستم ده هيسمحلهم انهم يعملوا maintain لل Internet Data Base بالكامل من غير اى مشاكل ، طب دلوقتى بقى المواقع دى كلها هنعمل فيها اى بقى ؟

قالك بس كل المواقع الموجودة دى انا هخلى فى حاجة اسمها
ال Parent Name Servers **ودول بيبدأوا ب dot .** ، قالك بقى ان ال dot ده
هيكون ال Parent Name Servers ، وتحت ال dot بقى انا هعملك hierarchical
system وهحطلك حاجة اسمها ال **Top Level Domains** ،زى ال .com ،
وزى ال org ، وزى ال net وغيرهم ، وتحت كل واحدة منهم ، هحطلك ال
domain بتاعك ذات نفسه ، زى مثلا yahoo.com و google.com وهكذا بقى

وبرضو نفس الحكاية بالنسبة ل net و org ، وتحت google.com هحطلك ال
subdomains بقى زى mail.google.com وزى images.google.com وتحت كل
subdoamin ممكن احط برضو subdomain تانية وهكذا بقى

فى لسه عندى مشكلة موجودة ، انت دلوقتى عمال
تقولى hierarchical system ، طب انت هتخزن المعلومات دى كلها فين بقى ؟
قالك بس انا هحط المعلومات دى كلها فى Central Data Base
موجودة حوالين العالم اسمها ال Root Servers ، ودول عبارة سيرفرات كل
وظيفتهم فى الحياة انهم يعملوا Maintain للداتا بيز بتاعت
ال Domain Name Services دى

طيب علشان بقى محدش يتحكم في ال Root Servers دى ، وعلشان
ميقولش ان فى دولة معينة هى اللى بتتحكم فى ال Root Servers دول

قالك بس احنا هنقسم ال Root Servers دول حوالين العالم ، يعنى نحط كام سيرفر فى امريكا وكام سيرفر فى روسيا وكام واحد فى فرنسا وهكذا

ممكن تكتب فى جوجل root servers وهيطلعلك ان عددهم 13 root server تحديدا بيبدأوا من حرف ال A لحد حرف ال M حسب ما ويكيبيديا بتقول وهتلاقى ان الغالبية العظمى منهم من ال root servers دى مبنية على ال bind

فى ويكيبيديا برضو هتلاقي ال Operators اللى هما المؤسسات او الناس اللى بيشغلوا ال Root Servers دى ، هتلاقى ان حتى الان فى جامعات هى اللى بتشغل ال root servers دى ، وهتلاقى كمان فى root servers اللى بتشغلها هى ناسا ، وفى برضو الجيش الامريكى للابحاث

دلوقتى بقى فى سؤال وهو ، هل تفتكر ان ال 13 root server دول يقدروا انهم يشيلوا كل ال Requests بتاعت الكرة الارضية او بتاع الانترنت Users اللى على الكرة الارضية

تخيل بقى الكام مليار مستخدم للانترنت ،هل بس 13 سيرفر هيشيلوا الكم الكبير ده كله من ال Requests دى ؟ اكيد طبعا شبه مستحيل حاجة زى كده

قالك طب علشان تحل مشكلة زى دى ، قالك بس ، فى كل setup من ال 13 سيرفر دول ، انا مش هحط سيرفر واحد ، لا دا انا هحط سيرفرات كتيرة جدا وهيخلوا السيرفرات دى كلها تشتغل وهيستخدموا Technology اسمها **anycast** ، وال anycast دى بتسمحلك ان يكون عندك مجموعة اجهزة او مجموعة سيرفرات ولما تيجى تطلب كل الاجهزة دى او السيرفرات دى ، فانت هتطلبها كلها عن طريق IP واحد بس ، وقبل ما انت هتخش انهى سيرفر فيهم ، اعتبر ان كأن فى حاجة كده واقفة على الباب هتشوف ال request بتاعك جى من انهى مكان بالظبط ، وتبعتك لاقرب سيرفر او لاقرب root server بالنسبالك ، او ممكن تقول ان ال IP ده هو اللى هيبعتك لاقرب سيرفر بالنسبالك ، وبدأ بقى بدل ما هو سيرفر واحد او مجموعة سيرفرات بتمتلكها دولة واحدة ، قالك بس انا هستخدم ال Any Cast ده ، وبدأوا انهم يعملوا Replicate لل Internet DNS Servers حوالين العالم

يعنى مثلا هما جم فى افريقيا وراحوا مختارين مثلا المغرب و جنوب افريقيا

وكذلك الامر برضو بالنسبة لقارة اسيا ، لو دخلت على الموقع ده

www.root-servers.org

هتلاقى عندك مثلا سيرفر موجود فى اسيا وهتلاقى واحد تانى Replicated منه فى افريقيا وهكذا

وبرضو فى الموقع ده موجود تحت ال ip address بتاع كل واحد فيهم ، يعنى مثلا ال A root Server الايبى بتاعه 198.41.0.4 وهتلاقى مع كل Root Server فيهم ال Site بتاع كل واحد ، يعنى مثلا ال A Root Server موجود فى 8 اماكن زى New York و London ، وكده بقت النسخة اللى موجودة عند دولة معينة ، بقت موجود منها نفس النسخة فى دولة تانية بالظبط ، وكل ده لسببين

الاول ان مفيش دولة تكون محتكرة الانترنت ، والحاجة التانية ان ال Servers دى بتكون Critical جدا ، بحيث ان لو حصل فى لحظة من اللحظات اى كارثة ، فيكون لسه عندنا فرصة اننا نأكسس ال resources الموجودة على الانترنت

يبقى كده عرفنا اننا عندنا حاجة اسمها DNS ووظيفته انه يحول الاسم ل IP ، طيب دلوقتى فى حاجة تانية اتعملت علشان تكون بس عارف اى اللى بيحصل حواليك ، احنا قولنا اننا عندنا ال . dot وتحت ال dot دى بيكون فى ال com وال org وال net وتحتهم بقى ال domains ذات نفسها وبعدها ال subdomains

قالك بس انا هعمل طريقة تانية لل DNS ، هيبدأ ب dot وتحت كل dot ال Country Code ، وبالمناسبة الطريقة الاولى كان اسمها Generic Top Level Domain

انما بقى الطريقة التانية دى اسمها Country Code Top Level Domain ، وفى الطريقة التانية دى ، قالك انا هدى لكل دولة حرفين اتنين بس يميزوا الدولة دى من اسمها

يعنى مصر مثلا هديلها **eg** وامريكا **us** وبريطانيا هتكون **uk** وهكذا ، وتحت كل واحدة منهم برضو حط ال domain بتاعك يعنى مثلا google.eg او helwan.eg وبرضو تحتهم هيكون ال Subdomains ، فكده بقى عندنا طريقتين لل DNS انه يشتغل بيهم ، او بشكل ادق مش طريقتين ، ممكن تقول ان فى

2 DNS Hierarchical Systems

بس كلهم فى الاخر بيلفوا ويرجعوا لل Root Servers اللى هما ال 13 سيرفر او ايا كان عددهم بقى وهما Replicated ، اه بالمناسبة ال www هى كمان عبارة عن subdomain

طيب دلوقتى بقى لو عندك مثلا web site وعايز توصفه ، هتوصفه ازاى ؟ قالك انت هتبدأ من تحت خالص لفوق ، مثلا اخر subdomain عندك هو ال www فانت كده هتبدأ بال www وبينه وبين ال Parent بتاعه حط . dot ، بالشكل ده

www.yahoo.com.

لحد ما توصل لل com وهيكون هنا ال parent بتاع ال com هو ال . dot ، بس استنى هنا ، انت اكيد هتسأل وتقول انك طول عمرك بتطلب المواقع بدون ما تكتب ال . dot اللى فى الاخر دى صح ؟ طبعا صح ، بس انت هنا مش هيفرق

معاك سواء انت حطيتها او محططهاش مش هيفرق ، لان كده كده ال browser اوتوماتيك بيضيفها ، لان الموضوع بالنسباله بقى من الحاجات البديهية

دلوقتى بقى لو جيت على جهاز ال Client ، وفتحت ملف ال hosts

cat /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

هتلاقى ان الملف ده بيكون فيه entries ، وكل entry بيكون فيها ال IP وقصاده بيكون الاسم

كذلك الامر برضو بالنسبة لل DNS ، هو عبارة عن شوية ملفات وكل ملف عبارة عن شوية entries وكل entry بتكون عبارة عن ال IP وقصاده الاسم ، ال DNS عبارة عن كده بالظبط متفتكرش يعنى ان ال DNS فيه اختراع

الحاجة اللى بعد كده هيكون عندك شوية tools كده ممكن تتعامل معاها زى ال **nslookup** ودى فايدتها انك تسأل ال DNS اللى عندك على عناوين المواقع ، يعنى مثلا لو عايز تعرف ال IP بتاع yahoo.com

nslookup yahoo.com

هيرد عليك بالشكل ده

Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: yahoo.com
Address: 98.138.219.231
Name: yahoo.com
Address: 98.138.219.232
Name: yahoo.com
Address: 72.30.35.9
Name: yahoo.com
Address: 98.137.246.7
Name: yahoo.com
Address: 72.30.35.10
Name: yahoo.com
Address: 98.137.246.8

اول حاجة هيقولك انه بيستخدم ال DNS اللى ال IP بتاعه هو 8.8.8.8 والبورت رقم 53

وبالمناسبة بقى ال DNS بي By Default بيستخدم البورت UDP 53 ، وتحت بقى بيقولك ان yahoo دى ليها العناوين دى Published على النت ، دى غير العناوين اللى بتكون على حسب الدول

يعنى مثلا google.com ليها ips بتختلف عن google.com.eg

طبعا انت لو كتبت بس فى الترمنال nslookup ودوست انتر هتظهرلك بالشكل ده وبالتالى ممكن تكتب اكتر من command بالشكل ده

```
[root@server ~]# nslookup
>
>
>
>
>
```

دلوقتى بقى لو عايز تخلى ال DNS بتاع جوجل هو ال DNS الافتراضى بتاعك ممكن تكتب كده

```
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
>
```

كده انا بسأل ال DNS بتاع جوجل على العنوانين بتاعت المواقع

فى برضو tool تانية اسمها dig ودى عبارة عن tool بتستخدمها علشان ت quary ال DNS ، بمعنى انها هتديك معلومات اكتر

```
[root@server ~]# dig redhat.com

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7 <<>> redhat.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54361
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;redhat.com.                    IN      A

;; ANSWER SECTION:
redhat.com.             2088    IN      A       209.132.183.105

;; Query time: 88 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Aug 03 16:43:53 EDT 2018
;; MSG SIZE  rcvd: 55
```

هنا بقى معلومات زى ال Quary Time ، يعنى الوقت اللى استغرقته الاداة دى علشان تسأل ال DNS على الايبى بتاع موقع redhat

وممكن تحس ان ال output بتاعت dig غريب شوية ، لكن بص فيه تانى هتلاقيه منظم ، مثلا عندك السطر ده

;; QUESTION SECTION:
;redhat.com. IN A

ده هنا بيقولك ان السؤال بتاعك هو ده وانت سألت على ال A اللى هو ال Address بتاع موقع redhat.com
وتحتها بقى عارضلك ال answer بتاع السؤال ده

; ANSWER SECTION:
redhat.com. 2088 IN A 209.132.183.105

هتلاقى عندك برضو السطر ده فى الاول خالص

flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

بيقولك انت سألت سؤال واحد ، وطلعتلك اجابة واحدة ، ومفيش فيهم اى authoritive name server ، وكمان مفيش اى additional information طلعتلك

بالمناسبة انت لما تيجى تستخدم ال dig ممكن تستخدم ال option اللى هو t– يعنى تسأله على ال type بتاع ال record اللى انت بتسأل عليه
ولو انت مدتلوش اى record type هو بيفترض انك عايز تجيب ال ip address بس ، **طب هى اى اصلا ال record type دى ؟**
بص ال record type دى معناها نوع ال DNS Entries اللى انت بتسأل عليها **اى بقى نوع ال DNS Entries دى هى كمان ؟؟** بص احنا قولنا ان ال DNS ما هو الا عبارة عن شوية ملفات او هو عبارة عن شوية معلومات
كل اللى بيعمله انه بي map الاسم لل IP بس كده ، طب هو اصلا المعلومات اللى بتتخزن دى هل هى كلها عبارة عن IP وقصاده الاسم ؟
لا طبعا ، ده انا ممكن استخدم ال DNS واقوله ان انا عندى service معينة وال service دى موجودة على ال IP الفلانى ده ، وبالتالى انا ممكن استخدم ال DNS فى استخدامات تانية كمان فى Advanced Usage

كده احنا لحد دلوقتى خدنا Introduction بسيطة عن ال DNS

بدأنا فى الفديو رقم 77 ، ده عبارة عن 12 دقيقة بس

البشمهندس مصطفى فى الفديو ده كان بيقول على ال Services اللى احنا المفروض ندرسها وهى

DNS

Bind DNS

Postfix

Dovecot

والاتنين دول اللى هما ال Postfix وال Dovecot عبارة عن ال Mail Services عندنا

ومن ضمن مواضيع ال DNS هى ال

Cashing Only Name Server

Master Server

Slave Server

وبيقول اننا وحنا شغالين مع ال Master وال Slave ، هنتكلم ان شاء الله عن ال

Forward Lookup

وال

Reverse Lookup

بعد بقى ما يخلص معانا ال mail server ، هيدينا ان شاء الله solutions جاهزة زى ال

iRedMail

وحاجة تانية زى ال

OpenFire

وده عبارة عن Chat System

كمان لسه عندنا شوية services تانية زى ال

Samba

PKI-PGP-GPG

xinetd Telnet, Printing CUPS,

Firewall

KickStart pxe

Selinux

SNMP

Nginx Server

وممكن ناخد حاجة علشان ال High Availability زى ال

Keepalived

علشان لو انت عندك service وعايز تعملها high availability

من اول بقى المرة الجاية هيكون التطبيق العملى ، هنحتاج سيرفرين لينكس وجهاز تانى علشان نعمل عليه test

11-BIND DNS Installation

من اول النهارده بقى هيكون عندنا سيرفرين ، واحد هيكون هو ال Primary Server ، والتانى هيكون هو ال Secondary Server ، والجهاز التالت ممكن يكون ويندوز او لينكس علشان نعمل منه test يعنى هتكون مجرد Client بس ، وافتكر اننا لما نقول ان هيكون عندنا جهاز client يعنى معناه اننا لازم نعمل لجهاز ال Client ده Configuration انه ياخد ال DNS Information من السيرفر اللى عندك ده اللى هو ال Primary Server ، بمعنى ان انت لو جيت فكرت اى اللى المفروض يحصل بالظبط ، فانت المفروض ان المكنة السيرفر دى او ال Primary Server ده او اللى اسمه Server-1 يكون معمول ليها configuration انها تعمل resolve من Public DNS على الانترنت او مثلا ال Open DNS او مثلا حاجة زى Google Public Server او غيرهم بقى حسب ما تحب ، معنى كده ان لما ال client يحب انه ي browse المواقع او انه يعمل resolve ، فهو لازم الاول يسأل ال Local DNS اللى عنده فى نفس ال Domain يعنى نفس المكان اللى هو موجود فيه ، وبعدين بقى ال Local DNS ده يروح يسأل ال Public DNS اللى على الانترنت

طيب فى حاجة عايز اقولك عليها وهى اننا لحد دلوقتى متكلمناش على اننا هنعمل السيرفر الاولانى او اللى هو ال Primary Server ده ك Authoritative DNS Server للشبكة الداخلية بتاعتى ، او بمعنى اخر ان ال DNS Server الاولانى اللى عندنا ده مفيش عليه اى Zone ، يعنى انا لسه معملتش اى دومين داخلى للشبكة بتاعتى دى
دلوقتى هو كل وظيفته انه هيستقبل ال Quary من ال User وبعدها هيروح يسأل الانترنت ، طيب حلو خالص

دلوقتى بقى السيرفر ده وهو بيستقبل ال quary من ال user ويروح يسأل الانترنت ، هل بقى فى اكتر من طريقة انه يشتغل بيها ؟؟ طيب بص يا سيدى دلوقتى لما ال Local DNS ده بيحاول انه يسال DNS تانيين او Public DNS دلوقتى بقى فى طريقتين علشان ال Local DNS ده يقدر انه ي resolve لل Client

الطريقة الاولى اسمها ال **Iterative Queries** ، والطريقة التانية اسمها ال **Recursive Quary** او **Recursive Lookup**

وبالمناسبة لما اقولك **resolve** او **query** او **lookup** فهما التلاتة حاجة واحدة ، معنى واحد يعنى ، التلاتة كده معناهم انى عايز اترجم الاسم ل IP او العكس انى عايز اترجم ال IP لاسم بالبلدى كده

طيب عملية ال Lookup امتى بتستخدمها ؟ بص انت بتستخدمها لما متكونش عارف اى النتيجة بالظبط ، بمعنى ان انت مش عارف اذا كنت هتقدر انك ترجع بنتيجة ولا لأ

ولما بقول Query ، فدى معناها ان ال Client هو اللى بيسأل السيرفر او سيرفر بيسأل سيرفر تانى ، وساعتها بقى الاسم الاشهر للعملية دى هى كلمة Query استعلام

انما بقى كلمة resolve ، معناها ان انت سالت وطلعلك نتيجة

يبقى كده كلمة Lookup معناها ان فى سؤال ، بس الله اعلم اذا كان هيكون فى ناتج ولا لأ ، اما resolve فمعناها ان فى سؤال وفى ناتج ، انما Quary فعادة بتطلق لما client يسأل سيرفر ، او سيرفر يسأل سيرفر تانى بس برضو انت مش متأكد الناتج هيكون اى بالظبط

لكن التلاتة مصطلح واحد ، وهو انك عايز تترجم الاسم لايبى او العكس

نرجع بقى لموضوعنا ، اى بقى موضوع ال Iterative Query وال Recursive Query ده بقى ؟؟ بص يا سيدى الموضوع بسيط جدا ، فاكر لما قولنا ان ال DNS بيبدأ بحاجة اسمها ال . dot او بمعنى اخر ال root server ، وقولنا ان ال root server ده ، مش سيرفر واحد ، لأ دول عبارة عن 13 سيرفر موجودين حوالين العالم كله وكل واحد منهم ، بيكون ليه replicated version منه ، وقولنا طبعا ان العالم كله بيعتمد على ال 13 root servers دول ، وكل عمليات ال resolving بتم عن طريق ال 13 root servers دول ، برضو هتسأل وتقول طب هما ال 13 سيرفر دول هيستحملوا الكلام ده كله ؟ هقولك فاكر لما قولنا انهم بيستخدموا تكنولوجى اسمها ال anycast ودى بتسحملك انه يكون عندك عدد معين من السيرفرات سواء بقى 10 سيرفرات او 50 سيرفر ، انه يكونوا كلهم واخدين نفس ال IP Address ، بس وانت جى عليهم ، يعنى وانت جى تسال ال 13 سيرفر دول فالراوتر بتاعك بيرميك على اقرب سيرفر ليه ، يعنى مثلا انت فى مصر وعايز تروح لل root server ، فانت اوتوماتيك هتروح لل replicated version اللى موجود عندك فى مصر او المغرب

وفاكر لما قولنا فى جزء ال Network ان ال unicast معناه One To One هنا بقى ال anycast معناه One To Nearest ، يعنى بتروح لاقرب DNS سيرفر بالنسبالك

طب ازاى بقى عملية ال routing بتم ؟

دى بقى متشغلش بالك بيها دلوقتى ، لان فى حوار كبير بخصوص ال anycast ده ، لو انت درست **CCIE** ان شاء الله هتلاقى ان موضوع ال anycast ده عبارة عن جزء كبير كده من منهج ال CCIE ، فانت ابعد عن الحوار ده دلوقتى كل اللى يهمك من ال anycast حاليا ، انك تبقى عارف ان بيكون فى مجموعة سيرفرات وكلهم ليهم نفس ال IP Address وال Client لما ياجى يعمل connect فالراوترات هى اللى بترميه على اقرب سيرفر بالنسباله

قولنا كمان ال 13 root servers دول بيبدأوا بحرف ال A وبينتهوا بحرف ال M ، وقولنا كمان ال root servers دى بيكون تحتها ال Top Level Domains زى ال com و net و org

وطبعا تحت كل واحد فيهم ال domain بقى ، زى redhat.com و google.com وطبعا تحت كل domain منهم ، فى عندنا ال subdomain زى www و mail وغيرهم ، لحد هنا والدنيا تمام

نرجع بقى لموضوعنا ، احنا دلوقتى لسه معندناش اى domain ولا اى حاجة خالص ، يعنى احنا اصلا بعاد عن الحاجات دى اللى ال . وال com والباقى

دلوقتى بقى انت روحت عملتلك Local DNS ، وفى وراء ال Local DNS ده شوية Clients عايزين يعملوا resolve ، دلوقتى بقى انت قولت لل Local DNS انت لما تحب تطلع او تسال ابقى روح اسأل ال DNS بتاع جوجل ، اللى هو ns1.google.com وال ns هى اختصار ل Name Server ، دلوقتى برضو انت عندك client راح يسأل ال Local DNS ويقوله قولى على ال IP Address بتاع www.redhat.com ، فال Local DNS ده هيروح يسأل ال DNS بتاع جوجل اللى هو مثلا ns1.google.com ، يروح ال DNS بتاع جوجل مثلا يرد على ال Local DNS ويقوله انه ميعرفش حاجة عن الموقع اللى هو عايز يعرف ال IP بتاعه لانه مش فى نفس ال Domain بتاعه ، ليه مش فى نفس الدومين ، ببساطة لان الدومين بتاع جوجل مثلا بالشكل ده

google.com

اما بتاع redhat فهو ليس subdomain من google.com وانما هو domain لوحده مستقل بالشكل ده

redhat.com

دلوقتى بقى ال DNS بتاع جوجل هيقول للLocal DNS روح اسأل ال dot . اللى هو ال root servers ذات نفسها ، ويروح بعدها ال Local DNS ياخد النتيجة من ال DNS بتاع جوجل ويبعتها للclient اللى طلب ، لكن هل انت كده رجعت للclient النتيجة اللى هو عايزها ، ولا رجعتله **reference** لحد تانى يسأله وهو ال root servers ؟

اكيد طبعا انت رجعتله reference لحد تانى يساله ، يروح بقى ال Client بذات نفسه يسأل ال root server ، ها يعم هل تعرف حد بالاسم ده

www.redhat.com

يروح ال root server يرد على ال client ويقوله انه ميعرفش حد بالاسم ده

www.redhat.com

لكن يقوله ان يعرف com ، ويروح مرجع ال result دى للclient مرة تانية ، يبقى للمرة التانية ال root server هيرجع هو كمان reference للclient ، يروح ال client مرة تانية يسأل ال DNS اللى مسؤل عن ال Domain اللى هو com ، وبرضو ال DNS ده اللى مسؤل عن com هيقوله انه ميعرفش حد بالاسم www.redhat لكن يعرف ال DNS اللى مسؤل عن ال domain اللى هو redhat ، يبقى كده للمرة التالتة ال DNS بتاع com هيرجع reference للclient هيرجعله بقى reference للDNS بتاع redhat ، يروح برضو ال Client يسأل ال DNS المسؤل عن redhat ولازم بنسبة 100% يكون ال DNS المسؤل عن redhat عارف عن ال www ، وطبعا بما انه هيكون عارف فهيروح رادد على

ال client ويقوله ايوه انه عارف انه عنده host او web site بالاسم www.redhat.com وال IP Address بتاعه كذا 209.132.183.105

من الاخر كده ال Iterative Quary معناها ان ال Client هيفضل يسأل ويتعب لحد ما يلاقى الناتج ، او ممكن ميلاقهوش اذا مكنش فى web site بالاسم اللى هو طالبه

يعنى بيفضل ياخد references لحد ما يوصل للناتج اللى هو عايزه ، وكل reference منهم عبارة عن نتيجة بتقربه للناتج اللى هو عايزه ، بس فى الاخر هو مش ضامن انه يلاقى host بالاسم ده

طيب العكس بقى ال recursive quary ، ال client هيروح يسأل ال Local DNS وبعدين ال Local DNS هو بعد كده اللى هيروح بقى يسأل ال root server وال root server يرد عليه ب reference لل top level domains ، وهكذا بقى لحد ما ال Local DNS يجيب النتيجة النهائية ويوديها لل Client

يعنى باختصار شديد فى عملية ال recursive quary ال Local DNS هو اللى هيتعب ويتفشخ لحد ما يوصل للنتيجة ويبعتها بعد كده لل client

طيب ده كده معناه اى بالنسبالك ؟؟ اولا لو انت شغال فى شركة هتقول انه اسهلك انه يكون فى مكنة واحدة وهى اللى تعمل ال recursive quary ده صح ؟ هقولك طبعا ايوه صح

لان انت المفروض طالما شغال فى شركة فانت المفروض تخلى عندك Local DNS بدل ما انت بتعذب ال Clients وال Local DNS ده هو اللى بيعمل recursive quary

دلوقتى بقى فى موضوع تانى ، هنفترض ان انت عندك Public DNS ، يعنى عندك سيرفر وادتله Public IP Address ، هل بقى تفتكر انه من الحكمة انك تخلى اى حد انه يستخدم ال Public DNS ده ؟ او انه مثلا يعمل recursive quary لاى حد فى الدنيا بمعنى ادق ؟
اكيد طبعا لأ لان هيكون فى Load كبير جدا على السيرفر ده

يبقى اذا لو انت عندك شركة المفروض تخلى ال Local DNS اللى عندك هو اللى يعمل ال recursive quary ، الحاجة التانية اللى لازم تحطها فى اعتبارك وهى عملية ال sizing
يعنى مثلا متروحش تجيب مكنة تعبانة ويكون عندك عدد كبير من ال client وتستخدمها ك DNS ، ففى الحالات اللى زى كده حاول انه يكون عندك

اتنين DNS Servers علشان توزع ال Load عليهم او 3 كمان ، مش هيزعلك فى حاجة

اخر حاجة بقى طالما انه هيكون عندك سيرفر او Local DNS ، هل بقى تفتكر انه من الافضل انه بدل ما ال Local DNS ده عمال كل شوية اى حد يسأله يروح يدور على النتيجة على النت وبعدين يجبهاله ، ولا انه اى حد طلب منه اى حاجة فالمفروض انه يخزنها عنده ولما ياجى اى حد تانى يسأله ميروحش يدور على النت بقى ، ويروح باعتله النتيجة على طول لانها متخزنة عنده ؟

اكيد طبعا الافضل ان ال Local DNS ده يخزن النتائج عنده ، وكده انا فى الحالة دى ممكن اعمل Extend لل Capability بتاعت ال Local DNS واخليه يعمل عملية Cashing

وعملية ال Cashing بكل بساطة معناها ان كل عملية resolve تتم ، اخلى ال Local DNS يخزن الناتج عنده ، وبالتالى لما ياجى يوزر يطلب url معين ، فال Local DNS يبعتله الناتج بسرعة

برضو عملية تخزين ال Cash ده او ال records دى مش بتتخزن الى ما لا نهاية ، لازم تاخد بالك من النقطة دى كويس اوى ، طيب ازاى الكلام ده ؟

بص دلوقتى بداية من ال root servers ومرورا بال Top Level Domains ، كل ال DNS Servers دى ، كل واحد منهم بيكون عامل لل records اللى عنده دى حاجة اسمها **TTL** ، اى بقى ال TTL ده ؟؟؟

بص ال TTL هى اختصار ل **Time To Live** ، ومعناها ان مثلا لما ال Local DNS يروح يسال ال Public DNS او ال Top Level Domains ، فهيردوا عليه ويقولوله انه ممكن يحتفظ بالعنوان ده لمدة 12 ساعة مثلا وبعدها ياجى يسأل ال Public DNS دى من تانى لو حب يعنى

فال TTL دى عبارة عن وسيلة علشان تتحكم فى الوقت اللى هيخزن فيه ال records دى قد اى بالظبط

انت ممكن تسال وتقول طب وليه يكون فى اصلا ال TTL دى ؟ بكل بساطة دلوقتى ال DNS اللى شايل الموقع اللى اسمه www.redhat.com دلوقتى بقى ال IP بتاعه مثلا كذا ، وجى بقى ال Local DNS خد ال IP بتاع الموقع ده من ال DNS الكبير ده ، وجه مثلا ال DNS اللى شايل الموقع ده حب انه يغير ال IP بتاع الموقع ده ، فاكيد كان لازم يكون فى حاجة اسمها ال TTL علشان لما ال Local DNS يسأل ال DNS الكبير ده ، يرد عليه بال IP الجديد ديما ، الموضوع شبه عملية ال lease time بتاعت ال DHCP اللى هو كل فترة معينة لازم تيجى تسال ال DHCP عن ال IP الجديد هيكون اي بالظبط

فى بقى عندك مجموعة من ال **DNS** كالتالى

Providers Tested

Let's compare them and see how fast they are from across the world. Those were the top 8 free DNS providers that we chose to evaluate:

Google 8.8.8.8: Private and unfiltered. Most popular option.

CloudFlare 1.1.1.1: Private and unfiltered. New player.

Quad9 9.9.9.9: Private and security aware. New player that blocks access to malicious domains.

OpenDNS 208.67.222.222: Old player that blocks malicious domains and offers the option to block adult content.

Norton DNS 199.85.126.20: Old player that blocks malicious domains and is integrated with their Antivirus.

CleanBrowsing 185.228.168.168: Private and security aware. New player that blocks access to adult content.

Yandex DNS 77.88.8.7: Old player that blocks malicious domains. Very popular in Russia.

Comodo DNS 8.26.56.26: Old player that blocks malicious domains.

طيب نرجع بقى لموضوعنا ، دلوقتى بقى ال Client لما يحب يكلم ال Local DNS هيكلمه على بورت UDP 53 ، وبرضو لما ال Local DNS يحب يكلم ال Public DNS هيكلمه برضو على بورت رقم UDP 53 ، طب وليه UDP ؟ ببساطة علشان عملية ال resolving تكون باسرع وقت ممكن

هنروح بقى لجهاز السيرفر اللى عندنا ، وبالمناسبة احنا عندنا اتنين DNS Servers هنشتغل عليهم ، الاول هنبدأ بالصعب

اول واحد هنشتغل معاه اسمه BIND DNS هو اسمه كده ، اسم ال DNS هو BIND

yum search dns

اهو

bind.x86_64 : The Berkeley Internet Name Domain (BIND) DNS (Domain Name System)

و BIND ده ممكن تعتبر هو اشهر DNS فى التاريخ كله

The Most Popular DNS Server In The History

وبالمناسبة ال Backbone بتاع الانترنت كله هتلاقيه قايم على BIND ده ، يعنى مثلا لو انت عندك ال 13 root server دول ، فانت عندك بتاع 9 او 10 منهم قايمين على BIND ده وهتلاقى مكنة واحدة بس فى الاخر هى اللى شغالة ويندوز

و BIND ده بينزل معاه شوية Packages مساعدة ليه ، تعالى اقولك على اسماهم

اول حاجة ال Package دى

bind.x86_64 : The Berkeley Internet Name Domain (BIND) DNS (Domain Name System)

دى لوحدها عبارة عن اسم ال Package بتاعت ال DNS Server نفسه ، بمعنى ان انت لو عملت install لل Package دى فكده هيكون عندك ال DNS Service ذات نفسها او بمعنى اخر هيكون عندك ال DNS ، وبالتالى ممكن تشغلها ك Service ذات نفسها

هتلاقى بقى معاها شوية Libraries خاصين مثلا بال 32 bit systems وفى برضو الخاصين بال 64 bit systems ، ومعاها كمان نسخة lite version وفى كمان ال Bind License

وفى برضو عندك Package تانية بالشكل ده

bind-pkcs11-utils.x86_64 : Bind tools with native PKCS#11 for using DNSSEC

ودى بتستخدمها لما تيجى تعمل DNS SEC ، وهى اللى بتستخدمها لما تيجى تعمل Signing لل Records بتاعتك لو انت هتشتغل DNS SEC

فى عندك برضو Package بالاسم ده

bind-utils.x86_64

اى بقى bind-utils دى ؟؟ دى عبارة عن package بتديك شوية utils تستخدمها ك Client وليس ك Server

فى برضو عندك Package تانية اسمها

bind-chroot.x86_64 : A chroot runtime environment for the ISC BIND DNS server

دى عبارة عن Package بتسمحلك انك تعمل chroot لل binaries
وال configuration بتاعت ال DNS Server ، بمعنى اخر كلمة chroot اصلا
معناها انى هحجز ال binaries وال configuration بتاعت service معينة
واخليها موجودة بمكان ما ، بحيث ان لو حد عمل اى attack عليها يكون
محجوز او ميقدرش انه يوصلها ، وال chroot فى بعض ال OS زى ال BSD
بيسموها هناك Gail يعنى سجن ، فهى بكل بساطة معناها انى بحجز
ال binaries او ال configuration files الخاصة ب service ما بحجزها فى مكان
مختلف تماما عن مكانها الاصلى

والمكان ده بيكون هو ال Parent بتاعها ، فا بيقولك انه يفضل جدا ان لو عندك
service معينة وتقدر انك تعملها chroot ، فاعملها ال chroot متستناش يعنى

تعالى بقى نعمل setup لل DNS ، ونعمله كمان chroot

اه بالمناسبة ال BIND ده عبار عن Implementation اول لل DNS ، عندنا بقى Implementation تانى تبع RedHat وبدأت انها تنزله من اول الاصدار رقم سبعة اسمه unbound

unbound.x86_64 : Validating, recursive, and caching DNS(SEC) resolver

وال unbound ده هو عبارة عن recursive و cashing DNS فى نفس الوقت طيب اى بقى الفرق بينه وبين BIND ؟ ال unbound بتستخدمه فى حالة ان انت عندك شبكة وعايز تعمل recursive lookup او cashing للشبكة دى بس

فلو انت استخدمت ال unbound ، فانت هتستخدمها علشان تعمل recursive lookup او تعمل cashing لل records اللى بتطلعلك من علي ال recursive lookup دى ، لكن مش هتقدر انك تعمل دومينز داخلية او حتى Public Domain تشتغل عليها ، فدى ى حد ذاتها مشكلة

تعالى بقى على جهاز السيرفر وسطب الكام Package دول

yum install bind bind-chroot bind-utils

بالمناسبة برضو ملفات ال configuration بتاع ال DNS موجودة فى المسار ده

ls /etc/named

وتضغط اتنين tab هيظهرلك الناتج بالشكل ده

[root@server ~]# ls /etc/named
named/ named.conf named.iscdlv.key
named.rfc1912.zones named.root.key

اذا الملف الرئيسى اللى فيه ال configuration بتاعت ال DNS هو الملف
named.conf

vim /etc/named.conf

هتقولى ازاى يعم ، ازاى بما اننا نزلنا ال Package اللى هى Chroot ، ليه بقى ملفات ال configuration ما راحتش فى مكان لوحدها كده ؟ هقولك بقى ان انت اللى المفروض تاخد الملفات دى وتنقلها فى المكان الخاص بيها

طيب هتلاقى عندك برضو شوية ملفات كده زى الملف ده

less /etc/named.iscdlv.key

هتلاقيه فيه شوية keys كده ، ملناش دعوة بيهم دلوقتى

وبعد كده هتلاقى عندك الملف ده برضو

less /etc/named.rfc1912.zones

هتلاقى بقى فى الملف ده شوية zones وهى جاية كده مع التسطيب ،وهتلاقى ال zones الموجودة دى موجودة لل Local Host وللل localhost.domain وهتلاقيها موجودة مرة لل IPv4 ، ومرة لل IPv6

فى عندك برضو ملف تانى

less /etc/named.root.key

برضو عبارة عن شوية keys رايحة لل root هنعرفها بعدين ولازم تراجع الفديو رقم 78 فى الدقيقة رقم 49

عندك برضو الملف ده

less /var/named/named.ca

عارف اى بقى اللى فى الملف ده ؟؟ مفاجأة ، اللى موجود فى الملف ده هو ال 13 root servers ، بالشكل ده

;; ANSWER SECTION:

.	**518400**	**IN**	**NS**	**a.root-servers.net.**
.	**518400**	**IN**	**NS**	**b.root-servers.net.**
.	**518400**	**IN**	**NS**	**c.root-servers.net.**
.	**518400**	**IN**	**NS**	**d.root-servers.net.**
.	**518400**	**IN**	**NS**	**e.root-servers.net.**
.	**518400**	**IN**	**NS**	**f.root-servers.net.**
.	**518400**	**IN**	**NS**	**g.root-servers.net.**
.	**518400**	**IN**	**NS**	**h.root-servers.net.**
.	**518400**	**IN**	**NS**	**i.root-servers.net.**
.	**518400**	**IN**	**NS**	**j.root-servers.net.**
.	**518400**	**IN**	**NS**	**k.root-servers.net.**
.	**518400**	**IN**	**NS**	**l.root-servers.net.**
.	**518400**	**IN**	**NS**	**m.root-servers.net.**

وكمان هتلاقى تحت كل سيرفر فيهم وقصاده ال IP بتاعه ، سواء IPv4 او IPv6

;; ADDITIONAL SECTION:

a.root-servers.net. 3600000 IN A 198.41.0.4
a.root-servers.net. 3600000 IN AAAA 2001:503:ba3e::2:30
b.root-servers.net. 3600000 IN A 192.228.79.201
b.root-servers.net. 3600000 IN AAAA 2001:500:84::b
c.root-servers.net. 3600000 IN A 192.33.4.12
c.root-servers.net. 3600000 IN AAAA 2001:500:2::c
d.root-servers.net. 3600000 IN A 199.7.91.13
d.root-servers.net. 3600000 IN AAAA 2001:500:2d::d
e.root-servers.net. 3600000 IN A 192.203.230.10
e.root-servers.net. 3600000 IN AAAA 2001:500:a8::e
f.root-servers.net. 3600000 IN A 192.5.5.241
f.root-servers.net. 3600000 IN AAAA 2001:500:2f::f
g.root-servers.net. 3600000 IN A 192.112.36.4
g.root-servers.net. 3600000 IN AAAA 2001:500:12::d0d
h.root-servers.net. 3600000 IN A 198.97.190.53
h.root-servers.net. 3600000 IN AAAA 2001:500:1::53
i.root-servers.net. 3600000 IN A 192.36.148.17
i.root-servers.net. 3600000 IN AAAA 2001:7fe::53
j.root-servers.net. 3600000 IN A 192.58.128.30
j.root-servers.net. 3600000 IN AAAA 2001:503:c27::2:30
k.root-servers.net. 3600000 IN A 193.0.14.129
k.root-servers.net. 3600000 IN AAAA 2001:7fd::1
l.root-servers.net. 3600000 IN A 199.7.83.42
l.root-servers.net. 3600000 IN AAAA 2001:500:9f::42
m.root-servers.net. 3600000 IN A 202.12.27.33
m.root-servers.net. 3600000 IN AAAA 2001:dc3::35

علشان بعد كده لما تيجى تعمل resolve ، تكون عارف توصل لل root servers الاول ، لان انت لو مش قادر توصل لل root servers ازاى هتعمل queries اصلا ، فانت بمجرد ما تعمل install لل Packages دى فال Packages دى هتخلى عندك شوية ملفات كده علشان على الاقل تعرف تشغل ال service

تعالى بقى نشغل ال Service دى ، وبالمناسبة ال Package اسمها bind ، انما ال service اسمها named

systemctl start named

systemctl status named

لو انت فاكر اننا قولنا اننا هنشغل **chroot version** من ال named ، وده معناها ان ملفات ال bind او ال named لازم تكون موجودة فى مكان غير المكان الاصلى بتاعها

وال Package اللى اسمها **named-chroot** او **bind-chroot** الاتنين واحد يعنى ال Package دى بقى هتعملك Install للملفات فى مكان تانى خالص

او بمعنى اخر هتشغلك ملفات ال bind او ال named من مكان تانى خالص ، طيب دلوقتى بقى من اول الاصدار RHEL 7 ، فانت لازم توقف ال service دى كلها

systemctl stop named

وكمان هتعملها disable فى حالة انها لو مكانتش disabled by default

systemctl disable named

هتقولى اى يعم اللى انت بتقوله ده ، اومال انا هشغل ال DNS ازاى بقى ؟؟؟؟ هقولك ثانية واحدة بما اننا هنشغله **chrooted** ، ففى اصلا binary موجود هو ده اللى هنستخدمه بدل ال binary بتاع named الاصلى ، ال Binary بتاع ال chrooted service اسمه named-chroot وليس named فقط

هتسال برضو وتقول طب انا هغير ازاى الاماكن بتاعت ملفات ال Configuration ازاى ؟؟ بص يا سيدى الجماعة ال Developers عملولك Script جى مع ال Package اللى هى ال bind موجود فى المسار ده

/usr/libexec/setup-named-chroot.sh

بكل بساطة انت هت run الاسكريبت ده فى الترمنال وتحددله انت عايز تعمل setup للل chroot environment فى المسار المحدد بالشكل ده وكمان هتقوله فى الاخر كده انك عايز تعمل enable للل chrooted environment بالشكل ده

/usr/libexec/setup-named-chroot.sh /var/named/chroot on

تعالى بقى اعمل

[root@server ~]# ls /var/named/chroot/
dev/ etc/ run/ usr/ var/

هتتفاجأ انه ظهر فى ال directory دى شوية directories هما عبارة عن نسخة مصغرة للل file system بتاعك وكل directory فيهم بقى فيها الملفات الخاصة بال service دى

وطبعا دى ظهرت لما انت استخدمت ال Script ده ، وكل اللى عمله الامر ده انه نقلك الملفات اللى انت محتاجها علشان تعمل setup للل DNS فى isolated environment
وخليهالك فى المسار ده

/var/named/chroot/

طيب وعلشان تكون برضو فى الامان اكتر ، ممكن تعمل mask لل service اللى اسمها named

systemctl mask named

وبعدها بقى تعمل enable لل named-chroot

systemctl enable named-chroot

systemctl start named-chroot

systemctl status named-chroot

كده احنا مشغلين ال DNS ومشغلينه كمان من خلال chrooted environment يعنى بدل ما كنا بنشغله من /etc ، لا دلوقتى بقينا بنشغله بالمسار اللى احنا حددناه بنفسنا

طبعا لو تاخد بالك اننا شوفنا نوعين من الملفات الخاصة بال DNS حتى الان النوع الاول هو ال Configuration File اللى هو كان هنا

less /var/named/chroot/etc/named.conf

والنوع التانى هو ال Data File زى الملف ده

less /var/named/chroot/var/named/named.ca

وال Data Files احنا شوفنا الكود اللى جواها وهو عبارة عن اسماء ال root servers

12-Cashing Name Server

طبعا فى المرة اللى فاتت احنا اتكلمنا عن ال DNS وال BIND وقولنا اننا المرة دى هنبدأ نتكلم عن ال Cashing Name Server وبعد كده هنتكلم ان شاء الله عن ال Master Server او ال Master Name Server وفى ال Master Name Server هنتكلم فيه عن ال Forward Lookup وال Reverse Lookup ، وبعد ما نخلص الجزء ده ان شاء الله ، هنتكلم على جزء ال Slave Server وبرضو ال Slave Server هنخلص فيه جزء ال Forward Lookup وال Reverse Lookup ، وجزء ال slave server هيكون جزء سهل ان شاء الله ، كل اللى هنعمله اننا هنقوله روح هات من ال Master الايبى الفلانى ، يبقى كده معظم شغلنا هيكون فى ال Master Server

طيب دلوقتى بقى الجزء اللى احنا عايزين نخلصه دلوقتى ، هو جزء ال Cashing Name Server ، وحتة ال Cashing Name Server دى سهلة جدا ، كل اللى عليك تعمله انك تعدل directive 2 او directive 3 وكلمة directive معناها **statement** او **Line** واحد او سطر واحد فى ال Configuration

طيب لو انت فاكر من المرة اللى فاتت اننا قولنا ان ملفات ال configuration كانت موجودة ديما فى /etc ، لكن بما اننا عملنا install لل Package اللى اسمها bind-chroot

فكده هى عملتلك عزل تام لملفات ال configuration وملفات ال Data الخاصة بال service اللى هى bind وخليتها فى مكان جديد خالص وهو

/var/named/chroot

وعملية العزل دى احنا بنعملها علشان ن Limit الاضرار اللى ممكن تحصل لل DNS لو حصل عليه اى عملية Hack

طيب انت دلوقتى علشان متتغلبطش وتروح فى مرة كده تعدل الملف اللى موجود فى etc بدل الملف اللى موجود var/named/chroot ، يبقى احسن ليك انك تمسح الملف اللى موجود فى etc ، وتعمل softlink من الملف اللى موجود فى var/named/chroot/etc بالشكل ده

rm -f /etc/named.conf

ln -s /var/named/chroot/etc/named.conf /etc/named.conf

وبالتالى انت كده ضمنت ان لو فى system admin تانى هياجى مش ضامن انه ميكونش عارف حتة ال chroot وتلاقيه راح عدل فى الملف الاصلى ذاته نفسه وبالمناسة الخطوة دى غير مطلوبة على الاطلاق ومش هتفيدك بحاجة ، لكن انت بتعملها علشان تحاول انك تتلاشى حدوث اى مشكلة ممكن تحصل

تعالى بقى نفتح الملف بتاعتنا

vim /var/named/chroot/etc/named.conf

طبعا فى ملحوظة تانية وهى ، حاول متخليش الملف ده كبير جدا ، بمعنى ان انت ممكن تستخدم ال include وبالتالى هتوفر كتير فى عدد الاسطر اللى فى ملف ال configuration الرئيسى بالشكل ده

include "/var/named/chroot/etc/myzones.conf"

وهكذا بقى ، ممكن تعمل اى ملف configuration لوحده ، وبعدها تبقى تعمله include

تعالى بقى نبص على اول السطور اللى موجودة فى الملف ده او اول ال directives فى الملف ده

```
options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; };
```

ال options دى هى اللى بتعرف ال general settings بتاع ال DNS ، عندك مثلا اول حاجة وهى انه بي listen على بورت 53 ، وفاكر لما قولتلك ان ال DNS عنده بورتين شغال عليهم

اول حاجة وهو البورت رقم UDP 53 وده علشان ال End User يقدر انه ي connect على ال DNS Server يعنى يحاول يستخدمه علشان يعمل resolve

وبرضو بيستخدم نفس البورت 53 بس TCP علشان ال Master Name Server يقدر انه يكلم ال Slave Name Server علشان يعمل حاجة اسمها

Zone Transfer

يبقى كده السطر ده

listen-on port 53 { 127.0.0.1; };

خاص بال End User ، يعنى ده البورت اللى ال END User هي Listen عليه ، وبالمناسبة بقى كل ال Machines بتاعت ال End User بيستخدموا البورت رقم 53 بي By Default علشان يكلموا ال DNS علشان يعملوا عملية ال resolve فاكيد مش من الحكمة خالص انك تروح تغير البورت ده ، لان مين من الناس هيعرف ان ال DNS غير البورت بتاعه

طيب هنا بقى فى السطر ده برضو انا قولتله انه ي listen على البورت ده ، قولت لل DNS Server انه يتصنت على البورت ده على اى حاجة جياله عن الطريق البورت ده ويبدأ انه يعملها عملية resolve بس انت هتعمل resolve من مين بالظبط ، بص بي By Default هتلاقى ال Settings بتقولك انه هيعمل resolve من ال Local Host بس ، يعنى انت هت listen ك DNS Server لل Local Host بس

من الاخر كده ال DNS جى Configured انه يعمل resolve لنفسه بس مش من نفسه ، خد بالك من النقطة دى كويس

دلوقتى بقى انا لو خليته يعمل resolve لنفسه كده انا استفدت اى بقى ؟ اكيد طبعا مستفدتش حاجة ، فا طبعا المفروض اقوله هو هي Listen على انهى IP Address كمان يعنى انا هقوله انه هي listen على ال IP Address بتاع ال DNS Server ذات نفسه ، بالشكل ده

```
options {
        listen-on port 53 { 127.0.0.1; 201.201.0.3;  };
```

ولاحظ ان فى semicolon بعد ما تكتب ال IP اللى هي Listen عليه وكمان فى Space قبل ما تقفل القوس ، اوعى تنسى المسافات دى علشان لو جيت عملت restart للل service ال service هت Failed منك

يبقى كده ال DNS هي listen لنفسه ، وطبعا هي Listen على ال Interface اللى ال IP بتاعه **201.201.0.3** ، معنى كده ان انت لو عندك DNS Server وعندك مثلا بتاع اربعة Interfaces ، مثلا واحد من ال Interfaces دى واصل بال Public Internet وواحد واصل بال Zone بتاع ال **DMZ** ، وواحد واصل بال zone بتاع ال **internal net work**
فانت ممكن تقوله انت يا DNS هتستخدم علشان ت Listen للل IP Addresses كذا وكذا بس
او للل IP Address الفلانى بس ، معنى كده ان لو فى user جايلك ، وال user ده جايلك على IP تانى خالص ، زى مثلا انه جاى عن طريق ال Public Internet ، هل ال DNS هيقدر انه يعمله resolve ؟ طبعا لأ

طيب انت ممكن تحددله IP زى ما قولنا او عدد معين من الايبهات ، او ممكن تريح دماغك خالص وتقوله any ، وال any ده عبارة عن Special Case او Special Statment ومعناها انه ي Listen على اى Interface عندك ، او بمعنى اخر انه هي Listen على اى IP يكون Configured عندك

يعنى من الاخر كده ال DNS ده هيبقى فى وضع ال waiting لاى Quary يجيله من ال IP ده او بشكل ادق من ال Interface اللى واخد ال IP ده

طبعا البشمهندس مصطفى بيقول انه عمره ما هيستخدم كلمة any خالص الا لجهاز واحد بس والجهاز ده عليه IP واحد بس

يعنى يكون عندك DNS Server ويكون واصل بيه Interface واحد بس وبالتالى هنا بقى ممكن يستخدم كلمة any وطبعا بما انه عادة معظم ال DNS Servers بيكون ليها اكتر من Interface فبالتالى الافضل انك تكتب ال IP بالظبط بس

بعد كده بقى فى السطر ده

listen-on-v6 port 53 { ::1; };

ومعناه انه هي listen على نفس البورت ، بس لل IPv6 ، وطالما انت عندك IPv6 فانت ممكن تحطه هو كمان بالشكل ده

listen-on-v6 port 53 { ::1; fe80::412b:9377:35eb:63fb; };

لكن بما انى معنديش او بمعنى اخر مش بنهتم بال IPv6 دلوقتى فاحنا هنتخطى النقطة دى دلوقتى

بعد كده بقى بيبدأ انه يعرفنى شوية حاجات كده ،

بالنسبة بقى للسطر ده

directory "/var/named";

معناه انه بيعرف ال DNS فين بقى ال directory اللى فيها ال Data بتاعتك او بمعنى اخر فين ال Data Directory بتاعتك ، بس خلى بالك ان المسار ده

/var/named

هو عبارة عن Equivalent للمسار ده

/var/named/chroot/var/named

خد بالك كويس من النقطة دى ، ان المسار اللى فوق هو هو المسار اللى تحت ، وليه قاله **/var/named** ، لانها ببساطة بقت chrooted دلوقتى ، وابقى ارجع برضو للفديو رقم 79 فى الدقيقة 30

المهم السطر اللى بعد كده وهو

dump-file "/var/named/data/cache_dump.db";

اى بقى ال dump-file ده ؟ بص دلوقتى لو واحد جى وطلب من ال DNS ده انه عايز يعمل query للموقع اللى اسمه facebook.com ، فال DNS بعد ما يروح يدور على ال IP بتاع الموقع ده ويجيب المعلومات ، هياخد بقى الناتج ده ويعمله عملية dump يعنى يخزنه فى الملف ده

/var/named/data/cache_dump.db

السطر اللى بعد كده

statistics-file "/var/named/data/named_stats.txt";

هو عبارة عن ال Statistics file الخاصة بالاباتشى ، زى مثلا عملية ال Query خدت وقت قد اى بالظبط وهكذا

السطر بقى اللى بعد كده

memstatistics-file "/var/named/data/named_mem_stats.txt";

هنا بقى بعض ال memory statistics الخاصة بال service ذات نفسها ، يعنى ال service دى خدت قد اى من الرام

بعد كده بقى السطر ده

allow-query { localhost; };

هنا بقى انا بقوله مين اللى يقدر انه يستخدمنى علشان يعمل query منى يعنى مثلا انا عندى ال DNS Server بتاعى والسيرفر ده ليه اكتر من Interface وطبعا كل انترفيس منهم بيكون واصل بشبكة مختلفة ، يعنى مثلا عندك Interface بيكون واصل بالشبكة اللى فيها السيرفرات اللى احنا بنسميها ال DMZ وواحد تانى واصل بال Public Network وواحد تانى واصل بال Internal Network اللى فيها ال End User

طيب دلوقتى بقى زى ما احنا عارفين ان ال Public Network هى اى حاجة خارج ال range ده

10.0.0.0

192.168.0.0

172.16.0.0

دلوقتى بقى ال DMZ هقوله انها موجودة فى ال range اللى هو

172.16.0.0/16

والشبكة ال Internal بقى الخاصة بال End Users هتكون موجودة مثلا فى ال range ده

10.0.0.0/8

هنا بقى انا ممكن اقول لل DNS ان اللى يقدر انه يعملك Query هما الناس اللى جايين من ال Internal Network بس ، فكده انا هقوله انه يعمل allow لل subnet دى بس وبالتالى اى حد من ال DMZ مش هيقدر انه ي query ال DNS ،وبكده انا ممكن ا Limit مين اللى يقدر يستخدمنى ك DNS عن طريق ال directive اللى اسمها allow-query دى

وزى ما انت شايف كده ان ال DNS جاى ب By Default انه بي Listen لنفسه وبي allow ال Queries لنفسه برضو ، يعنى من الاخر كد جى شغال ك Stand Alone DNS يعنى بيشتغل على المكنة اللى هو متسطب عليها فقط

دلوقتى بقى انا هنا لو عايزه ي listen لاى Network هقوله بالشكل ده

allow-query { localhost; 201.201.0.1/24; };

ومتنساش ال ; ال semicolon

وبالمناسبة انت ممكن تقوله هنا برضو any ، طيب دلوقتى بقى افرض انى عايز احط subnet تالتة ، عادى جدا اكتبها برضو ومتنساش ال ; ومتنساش كمان ان فى الاخر فى space قبل ما تقفل القوس

دلوقتى بقى انا هضيف directive جديدة واقوله انه هيسمح انه يعمل cash لمين بالظبط ، بالشكل ده

allow-query-cache {localhost; 201.201.0.1/24; };

وده معناه انه هيعمل cache لل results بتاعت الناس اللى فى ال range ده **201.201.0.1/24**

بعد كده بقى فى عندنا شوية directive تانية ، احنا مش محتاجينها خالص زى السطر ده

dnssec-enable yes;

انا هنا مش محتاج ال DNS SEC خالص دلوقتى ،وبالتالى انا ممكن احذفها دلوقتى ، او اسيبها براحتى ، وبرضو السطر اللى بعد كده

dnssec-validation yes;

وهو ال DNS SEC Validation ده هنبقى نجيله بعدين

وطبعا بالنسبة للسطر ده

recursion yes;

فانا اكيد هخليه لانى عايز ال DNS انه يعمل recursive lookup للناس اللى بتعمله Quary

فى بقى directive تانى وهى ال logging

```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
```

ودى بتحدد لل DNS Server ال logging بتاعته ، وكمان ال Channel بتاعت ال Logging اسمها ال default_debug وكمان هيخزن ال logs بتاعته جوه ملف اسمه

/data/named.run

وال severity بتاعته هتكون dynamic ، طيب دلوقتى ال severity دى عبارة عن جزء خالص بال Log Server وبما اننا لسه مخدناش ال log server فاحنا هنتخطاها دلوقتى

بعدين بقى فى الاخر خالص فى عندك ال statment 2 دول

```
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

اول سطر وده بيعمل include لل data بتاعت الملف اللى فيه ال Root Servers ،والسطر التانى بيعمل include لل Keys بتاعت ال Root Servers دى

فى عندك برضو statement تانية وهى

```
zone "." IN {
        type hint;
        file "named.ca";
};
```

وال zone اللى هى . dot دى ، هى عبارة عن ال Parent بتاع كل ال DNS اللى موجود فى الدنيا ، اصلا اصلا ال root servers كلهم بيشاوروا على ال . dot دى

وبيقولك كمان ال type بتاعها هو hint وكمان ال file بتاعها هو named.ca ، طب اى اصلا ال type اللى هو hint ده ؟؟؟ بص كمان شوية هنيجى نعرف ال zones بتاعت ال Master Server وساعتها هنبقى نيجى لل type ، يعنى احنا اصلا هنعمل zones بايدينا وهنشرح كمان انواع ال Zones دى هى كمان ، فا خلى الجزء ده كمان شوية

خلاص كده احنا خلصنا الملف بتاعتنا ده ، اطلع منه بقى

:wq

وبعدها بقى اعمل restart لل named-chroot

systemctl restart named-chroot

systemctl status named-chroot

بالمناسبة متنساش ان المسار ده

/usr/share/doc

فى Sample Files لاغلب ال Services اللى انت بتعملها install عندك ، فانت لو فى ملف configuration ناقص عندك ، ممكن تروح تجيبه من المسار ده

زى مثلا ملف ال named.conf

/usr/share/doc/bind/named.conf.default

بالمناسبة لازم تخلى بالك من موضوع ان الملف يكون مملوك لل owner اللى هو ال root لكن ال group لازم تكون هى named

كده انت لازم تعدل ال ownership وتعدل كمان ال Selinux Context ، وده فى حالة انك هتاخد نسخة من الملف ده من المسار

/usr/share/doc/bind/named.conf.default

بالشكل ده

restorecon -R /etc/named.conf

وبعدها

ls -Z /etc/named.conf

ولازم برضو ترجع للفديو ده علشان مهم جدا ، وخصوصا من اول الدقيقة رقم 42

كده انا بعد ما عملت restart لل service دى ناقصلى خطوة اخيرة وهى انى اخلى ال firewall يعمل allow لاى حد يعمل quary على البورت رقم 53

firewall-cmd --add-service=dns --permanent

firewall-cmd --reload

كده بقى انا جاهز انى اروح على المكنة بتاعت ال End User واعمل Query منها

هاجى بقى على ال setting واقوله انه يعمل resolve من ال DNS اللى هو 201.201.0.3 ، نفس الفكرة اللى انت بتعملها لما بتغير ال IP فى اللاب بتاعك او الموبايل

بس هنا هتقوله على ال DNS اللى انت عملته ، وبالمناسبة انت ممكن تعمل الكلام ده على جهاز ال client لو كان لينكس عن طريق ال nmcli

nmcli connection modify Wired ipv4.dns 201.201.0.3
nmcli connection down Wired
nmcli connection up Wired

تعالى بقى روح على ال browser بتاع ال client وجرب تفتح مثلا اى موقع

طيب بص فى حاجة مهمة هنا ، دلوقتى البشمهندس او احنا لما روحنا لجهاز ال client وجربنا فى ال browser اى موقع او حتى عملنا ping ، وجينا علشان نشوف ال logs بتاعت ال DNS ، قصدى يعنى علشان نشوف هل ال traffic ده بيعدى على ال DNS Server ده ولا لأ ، معرفناش الحقيقة نعرف ، لكن البشمهندس مصطفى استخدم طريقة تانية علشان يعرف اذا كان ال traffic بيعدى على ال DNS Server ده ولا لأ ، هو استخدم الامر ده

tcpdump -n udp dst port 53

طيب بص بقى شرح الكلام ده من تانى

دلوقتى انا عندى DNS موجود ، بس مش متأكد هل الترافيك بيعدى عليه ولا لأ فا احنا عندنا 3 طرق علشان تعرف اذا كان الترافيك بيعدى على ال DNS Server ده ولا لأ ، طيب دلوقتى بقى ال configuration بتاع ال DNS هو very customizable ان انت تقول لل DNS اعملى Log لكل Query يحصل عليك حرفيا ، مش كده وبس

دا انا هخليك تقسم ال Queries اللى جيالك فى ملفات مختلفة ، وهنعمل حاجة زى كده بايدينا بس دى مش موضوعنا النهارده ، ودى كده الطريقة الاولى

اما بقى الطريقة التانية انى اعمل dump لل data base ، او انى اعمل dump لل Memory اللى ال DNS ك service بيستخدمها علشان يعمل الكاش بتاعه ، مهو خلى بالك برضو ان كل ال caches اللى موجودة دى الخاصة بال DNS بيكون فى منها نسختين لما انت ت Configure ال Logs ، نسخة بتكون فى ال Memory ونسخة تانية بتكون فى ملف

والنسخة اللى فى ملف دى بتكون Optional ، انما بقى اللى فى ال Memory هتفضل موجودة فى ال Memory ، وبتضيع كل مرة انت بتعمل فيها restart لل service

والطريقة التالتة انى ابص للترافيك اللى جى لل Interface بتاع ال DNS Server ده ، فاحنا هنا استخدمنا utility اسمها **tcpdump** وقولتله انى هبص على البروتوكول اللى هو UDP وعلى ال destination port رقم 53

tcpdump -udp dst port 53

تعالى بقى وانت منفذ الامر ده فى الترمنال ، روح بقى على جهاز ال client وافتح مثلا اى web site ، وليكن www.google.com

هتلاقى ناتج ال command ده بالشكل ده

listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
11:28:57.802435 IP 201.201.0.7.51670 > 201.201.0.3.domain: 16113+ A? snippets.cdn.mozilla.net. (42)
11:28:57.802483 IP 201.201.0.7.51670 > 201.201.0.3.domain: 56570+ AAAA? snippets.cdn.mozilla.net. (42)
11:28:57.802975 IP 201.201.0.3.25495 > 192.33.14.30.domain: 63427% [1au] A? snippets.cdn.mozilla.net. (53)
11:28:57.803257 IP 201.201.0.3.14783 > 192.33.14.30.domain: 42648% [1au] AAAA? snippets.cdn.mozilla.net. (53)
11:28:57.816878 IP 201.201.0.7.50229 > 201.201.0.3.domain: 45080+ A? snippets.cdn.mozilla.net. (42)
11:28:58.603939 IP 201.201.0.3.45702 > 192.42.93.30.domain: 61214% [1au] A? snippets.cdn.mozilla.net. (53)
11:28:58.604139 IP 201.201.0.3.25643 > 192.42.93.30.domain: 27947% [1au] AAAA? snippets.cdn.mozilla.net. (53)
11:28:58.686624 IP 201.201.0.3.lanschool-mpt > 84.53.139.64.domain: 50206% [1au] A? snippets.cdn.mozilla.net. (53)
11:28:58.731239 IP 201.201.0.3.15626 > 84.53.139.64.domain: 26187% [1au] AAAA? snippets.cdn.mozilla.net. (53)
11:28:58.783504 IP 201.201.0.3.35983 > 84.53.139.64.domain: 20289% [1au] DNSKEY? mozilla.net. (40)
11:28:59.585512 IP 201.201.0.3.10140 > 184.85.248.65.domain: 29148% [1au] DNSKEY? mozilla.net. (40)
11:28:59.907941 IP 201.201.0.3.27151 > 192.31.80.30.domain: 38075% [1au] DS? mozilla.net. (40)
11:29:00.132876 IP 201.201.0.3.28991 > 192.55.83.30.domain: 58785% [1au] DNSKEY? net. (32)
11:29:00.328201 IP 201.201.0.3.26132 > 192.36.148.17.domain: 47628% [1au] DS? net. (32)

11:29:00.329267 IP 201.201.0.3.55997 > 192.36.148.17.domain: 63532% [1au] NS? . (28)
11:29:00.457701 IP 201.201.0.3.47584 > 192.42.93.30.domain: 16328% [1au] AAAA? drcwo519tnci7.cloudfront.net. (57)
11:29:00.458793 IP 201.201.0.3.12491 > 192.42.93.30.domain: 34417% [1au] A? drcwo519tnci7.cloudfront.net. (57)
11:29:00.546444 IP 201.201.0.3.menandmice-lpm > 205.251.194.154.domain: 6200% [1au] AAAA? drcwo519tnci7.cloudfront.net. (57)
11:29:00.547774 IP 201.201.0.3.51770 > 192.35.51.30.domain: 46186% [1au] A? ns-418.awsdns-52.com. (49)
11:29:00.548502 IP 201.201.0.3.51202 > 192.35.51.30.domain: 10232% [1au] AAAA? ns-418.awsdns-52.com. (49)
11:29:00.549435 IP 201.201.0.3.60316 > 199.19.56.1.domain: 27843% [1au] A? ns-1306.awsdns-35.org. (50)
11:29:00.550040 IP 201.201.0.3.19875 > 199.19.56.1.domain: 35835% [1au] AAAA? ns-1306.awsdns-35.org. (50)
11:29:00.550948 IP 201.201.0.3.32789 > 213.248.216.1.domain: 21844% [1au] A? ns-1597.awsdns-07.co.uk. (52)
11:29:00.551718 IP 201.201.0.3.43983 > 213.248.216.1.domain: 43487% [1au] AAAA? ns-1597.awsdns-07.co.uk. (52)
11:29:00.631949 IP 201.201.0.3.48110 > 205.251.198.244.domain: 46074% [1au] A? ns-418.awsdns-52.com. (49)
11:29:00.637660 IP 201.201.0.7.55072 > 201.201.0.3.domain: 8313+ A? www.google.com. (32)
11:29:00.637709 IP 201.201.0.7.55072 > 201.201.0.3.domain: 59008+ AAAA? www.google.com. (32)
11:29:00.638762 IP 201.201.0.3.64532 > 216.239.38.10.domain: 20088% [1au] A? www.google.com. (43)
11:29:00.638961 IP 201.201.0.3.12730 > 216.239.38.10.domain: 40312% [1au] AAAA? www.google.com. (43)
11:29:00.682085 IP 201.201.0.3.47238 > 205.251.197.202.domain: 1006% [1au] A? ns-1597.awsdns-07.co.uk. (52)
11:29:00.755051 IP 201.201.0.3.36063 > 205.251.194.229.domain: 2055% [1au] A? ns-1306.awsdns-35.org. (50)
11:29:00.855217 IP 201.201.0.3.38007 > 205.251.192.163.domain: 48500% [1au] AAAA? ns-1306.awsdns-35.org. (50)

طيب تعرف بقى هو ليه راح لل IPs دى كلها ؟؟ عارف ليه راح لكل الايبهات ، ببساطة ال DNS Server بتاعك هو اللى اتمرمط وراح سأل الاول ال root servers وفضل يمشى لحد ما راح للسيرفر اللى شايل الموقع اللى هو www.google.com

طيب تعالى كده افتح ملف ال configuration من تانى ، وهتلاقى فى سطر كده غريب شوية وهو

recursive yes;

السطر ده معناه انه بيقول لل DNS Server انه هيعمل enable
لل recursive queries ، يعنى معناها انه هو اللى هيطمرمط لحد ما يجيب الناتج لل user وبالتالى هتلاقى ان مجرد quary بسيطة بس خلت ال DNS يروح يدور لحد ما يجيب النتيجة ، وبالتالى احنا كنا بنقول ان عملية ال sizing هتكون مهمة جدا بالنسبالك
يعنى مثلا ميكونش عندك users كتير فشخ ، وتيجى تخلى ال DNS يشتغل على جهاز امكانياته تعبانة زى 2 جيجا رام والكلام الفارغ ده

كده الحمد لله ال Caching Name Server انتهى

13-BIND Logging

طيب احنا دلوقتى فى الفديو رقم 80 ، والفديو ده هو تكملة للفديو رقم 79 ، واخر حاجة كنا وقفنا عندنا هى ال Logs ، هنكمل بقى النهارده موضوعنا برضو عن ال Logs +

دلوقتى بقى ، انت ممكن تسأل سؤال ، وهو هل ممكن انى اخلى ال DNS Server يبعت ال Logs على المسار

/var/log/messages

على طول ؟ اكيد طبعا ممكن

المكان ده بقى يعتبر هو المكان الرئيسى بتاع ال logs بتاع السيستم بتاعك ، او بمعنى اخر هو ال common log بتاع السيستم

طب ازاى بقى اخلى ال DNS ي log كل حاجة بتحصل للمسار ده ؟؟ بص فى عندك utility كده اسمها **rndc** ، ودى عبارة عن utility بتسحملك انك تتحكم فى ال name server او فى ال DNS بمعنى ادق

man rndc

ممكن انى اقول لل DNS انه يعمل enable لل query log ، عن طريق الامر ده

[root@server ~]# rndc querylog

عارف بمجرد ما انت طبقت الامر ده ، كل ال logs اللى عندك هتتبعت فى المسار

/var/log/messages

روح بقى على جهاز ال client وجرب تعمل ping مثلا او تعمل اى عملية resolve ، وروح على جهاز السيرفر واكتب

tailf /var/log/messages

هتلاقيه جايبلك الرسالة دى فى وسط سطر من السطور

Aug 6 11:18:27 server named[1227]: query logging is now on

روح تانى بقى على جهاز ال client وجرب تعمل ping مثلا او تعمل اى عملية resolve ، وروح على جهاز السيرفر واكتب

tailf /var/log/messages

هتلاقى بقى ال logs بتتعرضلك ، طيب اصلا اصلا احنا قبل ما نعمل حاجة زى كده ، مكنش فيه اصلا logs بتتخزن فى ال syslog

وخليك بالك بقى ان العملية دى مجهدة جدا (عملية انك تحط ال logs فى ال /var/log/messages) ، ليه بقى مجهدة جدا ؟؟ هقولك ، تخيل ان انت عندك users كتير جدا وطبعا كل ال logs دى هتتخزن فى messages ، معنى كده انه هيكون disk intensive operation ، ولو عايز توقف موضوع انه يرمى ال logs فى messages ، فانت هتستخدم نفس الامر برضو

rndc querylog

وتروح تفتح الملف تانى ، هتلاقيه بيقولك ان ال query logging is now off

تعالى بقى ناخد الحتة اللى احنا كنا بنقول عليها اننا نخليها لفديو ال logs لما نجيله ، تعالى بقى افتح ملف ال configuration بتاع bind

vim /var/named/chroot/etc/named.conf

فاكر بقى السطر ده

```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
```

بص يا سيدى الناس اللى عملوا ال bind ، ناس بيفهموا جدا ، ازاى بقى يعم ؟؟ قالك بص هو ال logs بتاعت ال DNS دى هل كلها زى بعض ولا فيها حاجات مختلفة ؟؟

بمعنى اخر هل ال DNS ك Service ، هل لما ياجى ي log ، هي log كل حاجة مع بعض ؟؟ طب هو اصلا قبل ما ي log كل حاجة مع بعض ، او المفروض اصلا قبل ما تحط ال logs دى هل المفروض انك تخليها كلها فى ملف واحد

ولا المفروض تفصلها ؟؟ اكيد طبعا المفروض انها تتفصل ، ليه بقى ؟؟ لان انت عندك debugging logs خاصة بال service ذات نفسها ، يعنى خاصة بال application ذات نفسه وهو شغال اللى هو bind او بمعنى اخر خاصة بال Process ذات نفسها ، وال Logs دى بقى اللى بيحب يوصلها عادة هما ال Developers

وفى عندك برضو Logs تانية خاصة بال security ، مثلا لو انت مشغل ال DNS SEC وال DNS SEC ده بيعمل check على ال Key الخاص بكل record فى ال DNS قبل ما يعمله resolve

وممكن يكون عندك برضو logs خاصة بال End Users العاديين ، وايضا ممكن يكون عندك logs خاصة بال Network نفسها ، وبرضو ممكن يكون عندك logs خاصة بال errors اللى بتحصل

يعنى مثلا ال DNS وهو شغال ممكن يحصل فيه error معين ، فقالك بس انا هفصلك الدنيا دى كلها عن بعض ، وتعالى بقى ارتبلك الدنيا دى كلها واسمحلك ان انت تعزلهم فى ملفات مختلفة

زى مثلا ال queries اللى يتعملها resolve هتكون فى ملف ، وال errors هتكون فى ملف ، وهكذا بقى

تعالى بقى كده ناخد مثال ، ونحط ال query logs فى مكان لوحدها ونتعامل معاها

دلوقتى بقى لما الناس حبوا يقسموا ال logs دى فى ملف ال configuration ، قالك انا هعمل حاجة اسمها channels او بمعنى اخر categories ، كلمة channel اصلا ممكن تعتبرها مكان كلمة category ، طيب دلوقتى بقى لو عايز تعمل channel خاصة بيك ، عادى مفيش اى مشكلة خالص ، اعمل يعم channel وسميها مثلا ahmed او اى اسم ، وحط فيها اللى انت عايزه

تعالى بقى نعمل channel بالشكل ده وتسميها مثلا queries_channel ، وبعد كده قوله انت هتحط ال logs دى بتاعت ال channel دى فى انهى file بالظبط ، وممكن كمان اقوله اطبعلى الوقت ، وده معناه انه قبل ما يطبع ال queries دى ، هيطبع قبلها الوقت اللى كانت ال Query دى بتم امتى ، واكيد حاجة زى كده انت هتحتاجها

لان انت مثلا ممكن يكون عندك users بيفتحوا مواقع اباحية ولا حاجة ، فانت تجيبه وتقولى من خلال ال logs انه فتح موقع كذا الساعة كذا ، كمان ممكن اقوله انه هيطبع اسم ال category ، بعد كده بقى عندك حاجة اسمها ال severity ، ودى ممكن تكون يا اما log او warning او critical ، ولما نيجى لل log server ان شاء الله هتعرف اى هى ال severity

اللى هى درجة الاهمية بتاعت ال Logs دى وممكن تريح دماغك خالص وتكتبها dynamic ، وهو هيشوف ال severity بتاعتك اى بالظبط ، ويختارلها بقى ال severity المناسبة ليها

كده انا فاضلى خطوة واحدة وهى انى اقوله ال logs دى ، او ممكن اجى تحت كده واقوله انى عايز اعمل enable لل category بتاعت ال Queries ، واقولى بقى انهى channel هيجيب منها ،واديله بقى اسم ال channel اللى انا عملتها اللى هى اسمها queries_channel ، كده انا خلاص خلصت ، شكل بقى الملف هيكون كده

```
channel queries_channel {
        file "data/queries.log";
        print-time yes;
        print-category yes;
        severity dynamic;
    };
    category queries { queries_channel; };
```

بعدها بقى تعمل restart لل named-chroot

```
[root@server ~]# systemctl restart named-chroot
```

ممكن بقى تروح تتأكد ان الملف بتاع ال logs اللى انت عملته ، هتلاقيها ات create اوتوماتيك لما انت عملت restart لل service اللى هى named-chroot

[root@server ~]# ls /var/named/chroot/var/named/data/
named.run queries.log

تعالى بقى علشان تتأكد ان ملف ال queries.log بتاعك ده ، بيتخزن فيه ال queries اللى ال End User بيطلبوها

tailf queries.log

وروح بقى على جهاز ال client وافتح اى موقع او حاول انك تعمل resolve هتلاقى ان كل ال queries اللى بيطلبها ال users بتتخزن فعلا فى الملف ده

يبقى كده ال queries بس هى اللى هتتخزن فى الملف ده ، طيب افرض بقى انك دلوقتى عايز تحط ال security logs ، يبقى ضيف بقى ال severity بتاعت ال security بتاعتك
وهتحط ال category بتاعت ال security بتاعتك وضيفها عادى جدا ، طب ال query errors ، برضو حطها لوحدها وهكذا بقى ، اه وبالمناسبة فى عندك category اسمها notify

وال category دى اللى هى notify علشان لو انت عندك Master Server و Slave Server فهو هيخزنلك ال logs اللى ما بين الاتنين دول

لو جينا مثلا حللنا سطر log زى ده

06-Aug-2018 12:44:19.986 queries: client 201.201.0.7#56106 (www.google.com): query: www.google.com IN A + (201.201.0.4)

اول حاجة بيقولك انه يوم كذا 06-Aug-2018 فى الساعة كذا 12:44:19.986 وهنا بيقولك الوقت بالساعة والدقيقة والثانية والمللى ثانية ، بيقولك بقى ان ال client اللى هو ال IP بتاعه كذا client 201.201.0.7 وبي connect من البورت رقم كذا 56106 وال client ده حاول انه يعمل resolve للموقع ده

www.google.com

وال IP Address بتاع ال DNS Server اللى عمل resolve هو
كذا (201.201.0.4) + A ، طب هتقول هو ليه ال DNS او ال logs فيها رقم 4 اللى هو موجود فى اخر الايبى ده 201.201.0.4
هقولك فاكر لما قولنا ان دى عبارة عن recursive queries ، يعنى ال DNS ذات نفسه هو اللى بيتمرمط ويروح يجيب النتيجة

دلوقتى بقى انا عندى خازوق ، الملف ده هيخزن داتا قد اى ؟ يعنى مثلا تخيل ان انت عندك 10 الالاف مستخدم وال users دول بيستخدموا ال DNS ده ، هيبقى اى الحل مع ال Users دول ؟؟ طب انت عارف الملف ده ممكن حجمه فى اليوم الواحد يكون كام جيجا ؟ اكيد طبعا هيكون على حسب ال Queries ؟

فطبعا الموضوع هيكون صعب جدا عليك انك ت manage حاجة زى ، فا هيبقى اسهلك انك تتحكم فى الملف ده اللى هو ملف ال configuration الرئيسى بتاع ال named.conf

vim /var/named/chroot/etc/named.conf

واجى عند ال channel اللى احنا عملناها ، واقوله هو هيسيب كام نسخة من ملف ال logs اللى احنا عملناه ده ، ممكن اقوله كلمة versions يعنى معناها عدد النسخ وبعدها اكتب مثلا رقم 5 يعنى اعملى خمس نسخ من الملف ده ، وكمان هقوله ان كل نسخة من الملف ده هيكون مثلا حجمه 100 ميجا ، طبعا 100 ميجا ده حجم كبير جدا ، بالشكل ده

```
channel queries_channel {
        file "data/queries.log" versions 5 size 100m;
        print-time yes;
        print-category yes;
        severity dynamic;
    };
```

وبعدها بقى تعمل restart لل named-chroot

```
[root@server ~]# systemctl restart named-chroot
```

دلوقتى بقى بمجرد ما اول ملف يوصل لل 100 ميجا اللى انت حددتهوله ، هيبدأ انه ينقل على الملف التانى ، وهيحطلك فى اسم الملف الاول رقم 1 ، وهكذا بقى فى الملف التانى والتالت للاخر بقى

وبكده نكون خلصنا موضوع ال Logging لكن ارجع وافكرك ان دى مجرد اساسيات بسيطة

14-BIND CONT 1+2

احنا فى الفديو رقم 81 ، طيب لحد الدقيقة 20 من الفديو ده ، كان كله عبارة عن مراجعة على اللى فات ، بدأ بقى يتكلم عن ال DNS SEC وبيقول ان كل ال admins بيهربوا من حكاية ال DNS SEC دى ، لانها فعلا عبارة عن عملية مرهقة جدا جدا ، بيقولك بقى تخيل ان انت عندك DNS Server وال DNS Server ده وليكن عندك 20 zones طب ليه برضو ال DNS SEC ده مرهق ؟ لان انت وانت بت generate ال Keys فانت عادة بتخلى ال keys دى valid لمدة شهر وكل شهر انت المفروض تعمل regenerate لل keys مرة تانية

فغالبا ال System admins بيريحوا دماغهم ولا DNS SEC ولا قرف ، بس طبعا حاليا الناس اللى مسؤلين عن الانترنت حوالين العالم بيحاولوا انهم يعملوا Enforce لل DNS

طبعا بيقول انه هيعدى موضوع ال DNS SEC ده لحد ما يخلص موضوع ال core function بتاع ال DNS وهى عملية ال resolving وبعدها ان شاء الله هنبقى نخش على ال DNS SEC وده طبعا بعد ما نخلص ال Master Server وال Slave Server

طيب باختصار برضو علشان تفهم ال DNS SEC ، كل فكرة ال DNS SEC ان انت مع كل record هتضيفه لل DNS عندك انت هتخلى لل record ده key بحيث ان ال client لما يحاول انه يعمل resolve ل record معين عندك وليكن مثلا اسم ال record ده www.mydomain.com يلاقى ال Key بتاع ال record ده ،ولو بقى ملقاش ال record ده معمول ليه signed او مثلا مش موثق عن طريق ال key بتاع ال DNS Server بتاعه فهو اوتوماتيك بي mark ال query دى على انها invalid query ، عامل زى واحد واقف فى النصف وهو بيستقبل ال query منك وراح باعتلك result غير اللى انت مستنيها

طيب كل ده احنا لسه فى ملف ال configuration الرئيسى بتاع ال bind

vim /var/named/chroot/etc/named.conf

دلوقتى بقى عندك السطر ده

bindkeys-file "/etc/named.iscdlv.key";

بالنسبة لملف ال bindkeys ، فده ال DNS بتاعك بيستخدمه علشان يعرف ال record ده معمول ليه signed من مين بالظبط

لو جيت انت فتحت الملف ده اصلا

vim /var/named/chroot/etc/named.iscdlv.key

هتلاقى بقى فى الملف ده ال keys بتاعت ال root servers اللى موجودين حوالين العالم ، اى بقى اللى هيحصل عندك يا سيدى ؟؟ بص انت دلوقتى لو جيت تعمل Query على الموقع اللى هو مثلا www.mostafa.com والموقع ده اصلا عامل enable لل DNS SEC Feature ، فال DNS بتاعك بقى بيروح يشوف هل ال record ده اللى هو www.mostafa.com معمول ليه signed بواحد من ال keys دى اللى موجودة فى الملف ده ولأ ، وده باختصار شديد موضوع ال DNS SEC

نرجع بقى لملف ال configuration الرئيسى بتاعنا بتاع named.conf ، وطبعا هتلاقى تحت خالص سطر ال include ، والبشمهندس بيقول ان انت لو system admin ذكى فانت المفروض تستخدم ديما حوار ال include ده علشان يسهل عليك الدنيا

طيب دلوقتى بقى اى اللى المفروض تعمله بخصوص ال directive الخاصة بال Logging دى

```
logging {
	channel default_debug {
		file "data/named.run";
		severity dynamic;
	};

	channel queries_channel {
		file "data/queries.log" versions 5 size 100m;
		print-time yes;
		print-category yes;
		severity dynamic;
	};
	category queries { queries_channel; };
};
```

فانت مثلا ممكن تعمل كومنت للسطور دى ، وتروح تعمل ملف خارجى وتحط فيه كل ال configuration بتاعت ال logs وبعدين تيجى فى الملف الرئيسى وتشاور عليها ، وكذلك الامر برضو لما اعمل zones ، **وكلمة zone هى مرادفة لكمة domain**

تعالى بقى افتح الملف ده هو كمان

vim /var/named/chroot/etc/named.rfc1912.zones

اللى فى الملف ده هو عبارة عن تجميعة من ال zones ، او تجميعة من ال domains ، فانت بقى هتلاقى عندك بعض ال Predefined zones زى مثلا ال zone اللى اسمها localhost وزى برضو ال zone اللى اسمها localhost.localdomain ودول طبعا بيكونوا لل IPv4 ، وبرضو هتلاقى عندك zones لل IPv6

```
zone
"1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
0.0.0.0.ip6.arpa" IN {
        type master;
        file "named.loopback";
        allow-update { none; };
};
```

طبعا الحاجات دى كلها متكررة ، فانت هتسأل هو ليه فى zones لل localhost وليه فى zones بال IP Addresses ، اى بقى الكلام ده كله ؟؟؟

بص يا سيدى ال Zone دى

```
zone "localhost.localdomain" IN {
        type master;
        file "named.localhost";
        allow-update { none; };
};
```

اللى هى ال forward lookup ، يعنى انت بتسال بالاسم وهو بيرد عليك بال IP

انما دى

```
zone "1.0.0.127.in-addr.arpa" IN {
        type master;
        file "named.loopback";
        allow-update { none; };
};
```

ده اللى هو ال reverse lookup ، من IP لاسم

طبعا انت هتسال وتقول ، هو فيه اصلا services بتعمل العكس ؟ هقولك اه ان فى بعض ال services بتعتمد على ال DNS اعتماد كامل ، والمثال على كده هو ال Mail Service

انت بقى لما تقول لل mail service ان انت مثلا عايز تبعت ل mostafa@yahoo.com ، طب انت اصلا اصلا متعرفش ال Mail Server ده موجود فين بالظبط ، فانت فى الحقيقة بتقوله انك عايز تبعت للراجل ده @ الدومين ده ، فانت بقى فى الحالة دى هتحتاج انك تحول ال IP لاسم فى برضو بعض ال services التانية زى ال kerberose

فا زى ما انت شايف ان ال DNS بيعمل عمليتين دلوقتى ، الاولى وهى انه بيحول الاسم ل IP وده ال default اللى احنا محتاجينه اصلا ، والعملية التانية انه بيحول ال IP لاسم

يعنى مثلا تبقى انت عارف ال IP بس انت مش عارف الاسم اي ، فانت هنا بقى هتسأل ال DNS وهو هيعملك عملية reversed query ، وخلى بالك اوى من كلمة reversed دى

خلى بالك انه فى فرق كبير فشخ بين كلمة **recursive** وبين كلمة **reversed**

يعنى احنا اصلا دلوقتى لو اتكلمنا عن انواع ال Queries ، فاحنا عندنا نوعين الاول وهو ال iterative query والتانى هو ال recursive query

ال **recursive** انت بتروح تسأل ال **DNS** بتقوله فين عنوان الموقع الفلانى فهو بقى يروح يعدى على كل ال **DNS Servers** اللى موجودة فى ال **chain** دى فى السلسة دى يعنى من اول ال **root servers** لحد ما يجبلك الناتج النهائى ، يعنى من الاخر كده ال **DNS** هو اللى بيتمرمط

انمابقى ال **reversed query** فهى عبارة عن نوع ال **Query** اللى بتقوله انا معايا ال **IP** بس عايز اعرف الاسم

انما ال **forward** بتقوله ان انا معايا الاسم وعايز ال **IP**

Iterative Query VS Recursive Query ======= Forward Lookup VS Reversed Lookup

بدأنا بقى فى الفديو رقم 82

وهو عبارة عن مجرد تكملة بسيطة للفديو رقم 81 ، واحنا لسه فى الملف ده

vim /var/named/chroot/etc/named.rfc1912.zones

بص بقى يا برنس ، من ضمن الحاجات اللى انت لازم تحطها فى اعتبارك ان انت لما تعمل اى domain عندك على السيرفر ، فانت المفروض ان ال records اللى تكون عندك فى الحالة الطبيعية
ان انت هتعمل اتنين zones ، ال Zone الاولى علشان تعمل ال forward Queries او ال Forward Lookup اللى هو تحول الاسم ل IP ، وال zone التانية اللى هى ال Reversed Queries او ال Reversed Lookup يعنى تحول ال IP لاسم

الشرح من تانى ، دلوقتى لو انت عندك دومين ، دلوقتى بقى فى الحالة الطبيعية بتاعتك وانت شغال ك System admin لما تيجى ت configure الدومين ده فى ال DNS ، فااصلا فى الحالة الطبيعية انت ممكن تعمل ال forward lookup بس ، لكن انت المفروض انك تعمل الاتنين ، تعمل ال forward lookup وال reversed lookup علشان تحول من اسم ل IP والعكس

وبالتالى انت علشان تحول من اسم ل IP لازم تعمل ال forward lookup zone
وعلشان تحول من IP لاسم يبقى لازم تعمل ال Reversed Lookup Zone

طبعا انت مش مجبر خالص ، يعنى ممكن تعمل forward lookup Zone بس
وممكن تعمل reversed lookup zone بس ، لكن الافضل انت تعمل الاتنين ،
وانت هتلاقى ان الغالبية العظمى من ال System admins عاملين ال Forward
Lookup بس ، ولكن خليك فاكر ان فى بعض ال services لازملها ال Reversed
Lookup زى ال Mail Service مثلا ، فانت اصلا من غير ال reversed lookup ال
mail service مش هتشتغل عندك

دلوقتى بقى لما تيجى تعرف اى zone فى الدنيا ، فال Syntax بتاع ال Zones
دى واضح جدا ، اول حاجة هتكتب كلمة zone وبعدها بقى هتقوله اسم ال
Zone دى وليكن مثلا اسم ال zone دى mostafa.com اللى هو اسم ال domain
بتاعك ، وبعد ما تقول اسم ال Zone ، هتقوله بقى اى ال Class اللى ال Zone
دى موجودة فيها ، دلوقتى بقى كل ال Classes اللى احنا شغالين عليها
النهارده اسمها Internet Class او اختصارا IN

بعد كده بقى تفتح قوسين ، ومتنساش ال ; semicolon ، وبعدين هتقوله نوع ال Zone دى وهى موجودة على السيرفر بتاعك ، يعنى هل السيرفر بتاعك ده master server ولا slave server ، بعد كده بقى هتقوله فين الملف اللى هتحط فى ال records بتاعت ال DNS ، اخر حاجة خالص فى شوية Options ممكن تضيفها

تعالى بقى احنا نجرب syntax فى ملف فاضى خالص

vim test

```
zone "dns.com" IN {
        type master;
        file "test.forward";
        allow-query { 201.201.0.1/24;  };
};
```

كده احنا عملنا ال forward lookup zone

طيب دلوقتى بقى لو عايز تعمل ال reversed lookup zone ، فأول سؤال المفروض تسأله ، اى هى ال subnet بتاعت ال zone دى ؟؟

فانت مثلا ممكن تقول ان ال subnet بتاعت ال zone دى هى

201.201.0.1/24

حلو دلوقتى بقى لما اجى اعمل ال reversed lookup zone دى هتتعمل ازاى بقى ؟

بص يا سيدى انت اولا هتكتب الاسم المعكوس بتاعت ال zone دى او بشكل ادق المعكوس بتاعت ال subnet دى لل zone دى

طب اى بقى المعكوس ده ، بص يا برنس اولا انت ال subnet بتاعتك هى 201.201.0.1/24 ، بص بقى فين ال last octet هنا ؟ اكيد طبعا رقم 1 اللى هو الاخير ده ، تمام كده

بص دى بقى انساها خالص دلوقتى ، انسى ال last octet دى ، دلوقتى بقى اي اللى ثابت عندى من ال subnet دى ؟ اكيد طبعا هتقولى 201.201.0 ، تمام مظبوط

فانت بقى لما تيجى تكتب اسم ال reversed zone ، انت هتكتب الجزء الثابت من ال IP او من ال Subnet دى بس هتكتبها معكوسة

وبعدها بقى هتبدأ تكتب باقى الحاجات اللى تبع ال zone دى ، زى مثلا ال type هيكون master وهكذا بقى ، يعنى ال reversed zone هتكون بالشكل ده

```
zone "0.201.201.in-addr.arpa" IN {
        type master;
        file "test.reversed";
        allow-query { 201.201.0.1/24  };
};
```

بص بقى حتة ال **in-addr.arpa** دى هى عبارة عن ان الجزء ده بقى ثابت طب اى بقى **in-addr.arpa** ده ؟؟؟ بيقولك انهم حبوا يكرموا ال arpa net ففضل ال syntax ده موجود من اول ما ال DNS اتعمل لحد النهارده ، طب انت عارف اصلا هى اى ال ARPA Net دى اصلا ؟؟ طيب بص مبدئيا كده ال ARPA دى هى اختصار ل

Advanced Research Project Agency

وترجمتها كده ممكن تقول عليها بالبلدى كده انها وكالة الابحاث المتقدمة التابعة لوزارة الدفاع الامريكية ، وهم دول اصلا اللى عملوا النت فى البداية

فده طبعا كتكريم ليهم يعنى ان اسهم اتحط هنا ، فالجزء ده بقى اللى هو . in-addr.arpa معناها ان ده reversed address تبع ال arpa addresses وفضل لحد النهاردة بالشكل ده متغيرش

وبكده احنا دلوقتى قادرين اننا نعمل ال forward lookup zone وال reversed lookup zone ، وتقريبا كده انت خلصت جزء كبير جدا من ال DNS ، بمعنى اخر كده الجزء التقيل فى ال DNS خلص

تعالى بقى نصعب الامور شوية ، دلوقتى بقى لو قولتلك اننا عايزين نعمل zone ل subdomain او بشكل ادق بما ان ال zone هى هى ال domain ، فاحنا عايزين نعمل subdoamin بالاسم ده

test.ahmed.com

وال subdoamin ده شغال على ال subnet اللى هى

10.15.0.0/24

هتعملوا ازاى بقى ؟؟ بسيطة جدا بالشكل ده

```
zone "test.ahmed.com" IN {
        type master;
        file "test.forward";
        allow-query { 10.15.0.0/24;  };
};
```

برضو من ضمن ال best practice وهى انك حاول تخلى اسم الملف ي match اسم ال zone وطبعا حط برضو كلمة forward علشان تعرف اذا كان ده forward zone ولا لأ

ولو عايز تعمل ال reversed zone ، هتبقى برضو بسيطة بالشكل ده

```
zone "0.15.10.in-addr.arpa" IN {
        type master;
        file "test.reversed";
        allow-query { 201.201.0.1/24;  };
};
```

خلى بالك هنا ان اسم ال zone فى ال reversed هيكون بيبدأ من خلال ال subnet اللى ال subdoamin موجود عليه ، بمعنى ان انت مش هتكتب اسم ال domain فى ال reversed zone

لا لا انت هتكتب الجزء الثابت من ال IP بتاع ال Subnet اللى ال subdoamin ده شغال عليه ، اوعى تتلغبط فى الجزء ده

كده احنا خلصنا الفديو ده ، لكن بداية بقى من الدقية العشرين ، الكلام اللى جى كله عن ال reverse proxy

فى نقطة تانية ، دلوقتى انت لما تيجى تتكلم عن ال DNS ، هل انت محتاج انك تعمل **failover** مع ال DNS اصلا ؟؟ يعنى ال DNS ك Service هل انت محتاج لها failover ؟؟

وبالمناسبة انا مليش دعوة بال role بتاعتك هل انت Master ولا Slave ، انا مليش دعوة بالنقطة دى اصلا ، احنا بنتكلم على هل انت محتاج اصلا انك تعمل failover مع ال DNS ؟

الاجابة باختصار شديد جدا لأ طبعا ، انت مش محتاج اصلا failover ، ليه بقى ؟؟ لان انت لو جيت بصيت على اى Client فى الدنيا هتلاقى ان اى ك client ممكن تحطله اكتر من name server فى نفس الوقت

واكيد انت عارف ده كويس ، لما بتيجى تغير ال IP عندك فى الموبايل بتكتب ال DNS الاول وهو 8.8.8.8 والتانى وهو 8.8.4.4

فهل بقى تفتكر ان ال DNS ك Service محتاجة Failover اصلا ، وبالتالى طبعا انت ممكن ت configure اجهزة ال client انهم يستخدموا اكتر من DNS Server بحيث ان لو الاول وقع يبقى التانى موجود يحل مكانه وهكذا بقى

طبعا دلوقتى بقى فى فرق لو انت عايز ان ال service دى تكون highly available وتريح دماغك ، طيب دلوقتى بما انك عملت ال configuration على السيرفر الاولانى
يعنى مثلا فرضنا ان انت عندك سيرفرين فى الشبكة ،وانت سطبت ال DNS وعملتله configure على السيرفر الاولانى ، هل بقى انت محتاج انك تعمل replicate لل setup اللى انت عملته للسيرفر الاول وتعمله للسيرفر التانى يعنى هل كل حاجة انت عملتها فى السيرفر الاولانى ، هل بقى لازم تروح تعمل كل حاجة فى السيرفر التانى هو كمان

بمعنى اخر انت مثلا عملت zone 20 على السيرفر الاولانى ، وجيت انت عايز تضيف سيرفر جديد عندك فى الشركة ، هل بقى لازم انك تروح تكتب كل ال zones من اول وجديد وكل ال data files على السيرفر الجديد اللى انت ضفته ده ؟؟؟

اكيد طبعا لأ ، كل اللى هتعمله ان انت هتخلى السيرفر الاولانى زى ما هو وهتروح للسيرفر التانى ده وتخليه انه يكون slave server للسيرفر الاولانى وبالتالى هو لما يكون slave ، هيروح بقى للسيرفر الاولانى ويقولى ادينى كل ال zones اللى عندك دى او بمعنى اخر ادينى ال data files بتاعت ال zones اللى عندك دى ،وهيروح بقى يعمل لل zones دى download او بمعنى اخر يعملها حاجة اسمها Zone Transfer وبالتالى مع عملية ال zone transfer دى هيروح منزل ال Data Files ويبدأ بقى انه يشتغل عليها ، فال Slave هنا ما هو الا وسيلة توفر عليك وقتك ومجهودك

وبالتالى انت لو جيت عدلت فى ال Master Server ، كل اللى انت هتعمله انك هتعدل حاجة اسمها ال Serial Number بتاعت ال Zone اللى موجودة على ال Master Server واوتوماتيك اول ما تعدل ال Serial Number ، ال Master Server هيروح يعمل Notify لل Slave Server ويقوله ان فى Update عنده حصل وخد بقى ال Update ده

بص انت ممكن تحس ان الموضوع فى صعوبة شوية ، بس ده عادى لسه قدامك وقت فى موضوع ال DNS ده

15-BIND CONT 3

بدأنا فى الفديو رقم 83 ، وزى ما قولنا المرة اللى فاتت ان ال Setup بتاعنا هيكون اننا هنجرب الاول ال Master Name Server ، ولو فاكر من المرة اللى فاتت اننا هنبدأ نعمل DNS Zone ، وبعد ما نعمل ال DNS Zone دى ، هنبدأ بقى اننا نحط ال Settings بتاعتنا ، طيب علشان بقى تقول ان انت عندك DNS Zone فى حاجتين انت محتاجهم

اول حاجة ال configuration هتكون فى ملف ال named.conf ، كده انت هتروح فى ملف ال configuration الرئيسى اللى هو named.conf وتعرف ال Zone دى زى اسم ال Zone مثلا والنوع بتاع ال Zone دى ، يعنى هل انت هتعمل ال Zone دى ل Master Server ولا هتعملها ل Slave Server وبعد كده الملف اللى هيتخزن فيه ال records بتاعت ال DNS بتاعك وبعد كده مين اللى هيعمل Query من على ال zone او هيعمل Query لل Zone دى وممكن بقى تضيف Options زى ما انت عايز

الحاجة التانية بقى روح عرف ال data او الملف او ال records بتاعتك فى الملف اللى انت عرفته فى ال Zone لما عملتها اللى هو ده
(بعد كده الملف اللى هيتخزن فيه ال records بتاعت ال DNS بتاعك)

يعنى انت هتيجى فى ملف ال named.conf وتقوله ان انت عندك ملف فيه ال records والملف ده موجود فى المسار مثلا

/var/test.txt

فانا بقى هروح للملف ده اللى هو test.txt واحط كل ال records جواه ، وال record اصلا هو اسم ال domain ، يعنى انت هتكتب ال record وهتكتب قصاده ال IP او العكس

215.154.64.88 yahoo.com

طبعا الموضوع مش بالسهولة دى ، بس لسه فى شوية حاجات هنتكلم عنها بس بكل بساطة ده اللى احنا محتاجين نعمله

يبقى انا كده لازم اروح اعرف فى ملف ال configuration ال Parameters بتاعت ال Zone ، والحاجة التانية وهى انى لازم اروح اضيف ال records بايدى ، يعنى مثلا انا عندى سيرفر اسمه www وطبعا السيرفر ده ليه IP ، فانت بقى لازم تروح تعرف الكلام ده كله بايدك ، وخليك فاكر برضو ان ملف ال configuration بيكون فى ملف وملف ال records او ملف ال data بيكون فى مكان تانى خالص

طبعا متنساش ان ملف ال configuration بتاعت bind موجودة فى

/etc/

انما بقى ملفات ال data بتكون موجودة فى

/var/named

وبالتالى لما تعمل اى zone ، ملفات ال zones دى هتكون موجودة فى

/var/named

وطبعا يعنى زى ما انت عارف ان BIND هى اسم ال Package انما named هى اسم ال service

فى ملحوظة عايزك تخلى بالك من المسار ده علشان فيه ال sample configurations بتاعت bind

cd /usr/share/doc/bind-9.9.4/sample/

طيب دلوقتى بقى البشمهندس قعد كام دقيقة كده يظبط فى ملف ال configuration الرئيسى بتاع named.conf ، كل اللى عمله انه مسح ال comments اللى كانت فى الملف وبعدها بقى قال انه هيبدأ يعمل zone

تعالى بقى افتح الملف ده

vim /var/named/chroot/etc/named.conf

واعمل zone بالشكل ده

```
zone "ahmed.com" IN {
        type master;
        file "/var/named/ahmed.forward";
};
```

كده بقى احنا هنروح للملف ده اللى هو

vim var/named/chroot/var/named/ahmed.forward

خلى بالك بقى من النقطة دى وهى بما انك مشغل ال chroot ، فالمسار ده اللى هو

/var/named/

معناه المسار ده

/var/named/chroot/var/named/

وبكده انت تنسى المسار بتاع السيستم الرئيسى بتاعك

تعالى بقى روح للمسار ده

cd /var/named/chroot/var/named/timon.forward

cp named.localhost timon.forward

وتعالى بقى افتح الملف ده

vim timon.forward

هتلاقيه بالشكل ده

```
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
```

اول حاجة فى الملف ده وهو ال **TTL** اختصارا ل **Time To Live** وهى عبارة عن ال **Cache Time Value** ، وهيكون Day 1

وبعد كده بقى اى سطر هتحط فيه ال @ هيكون معناه الدومين بتاعك

واللى بعدها هى ال IN وهى ال Internet Class ، بعد كده بقى ال **SOA** وهى اختصار ل Start Of Authority ومعناها ان السيرفر ده هو ال Authoritative DNS لل Zone دى

باختصار هو ال DNS Server المسؤل عن ال Zone دى ، اللى بعدها بقى علامة ال @ التانية ، ودى معناها انك المفروض تمسحها وتحط مكانها اسم ال name server او ال dns اللى مسؤل عن ال zone دى ، طيب دلوقتى بقى ، لو انا اسم ال name server بتاعى هو ns0.ahmed.com ، يبقى انت هتحط الاسم زى ما هو بالشكل ده

والاسم اللى بعد كده هو اسم ال admin اللى مسؤل عن ال domain ده ، **وبالمناسبة انت لما تيجى تتعامل مع ال DNS متنساش ان اى اسم بتكتبه بيكون فى . dot فى الاخر ، لازم تاخد بالك كويس من النقطة دى كويس**

دلوقتى بقى لو عندك admin اسمه

admin@ahmed.com

فالاسم مينفعش يتكتب بالشكل ده ، لا انت هتكتبه كده

admin.timon.com.

كل اللى انت عملته انك شيلت علامة ال @ وهتحط مكانها dot ، يبقى ده كده الايميل بتاع الادمن اللى مسؤل عن الدومين ده.

بعد كده بقى فى الخمسة Parameters دول

0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H) ; minimum

ودول هنتكلم عنهم لما نيجى نعمل ال slave server

بعد كده بقى لازم تعرف ال Name Server اللى عندك وهيكون كده مثلا

ns0.ahmed.com.

ومتنساش ال . dot اللى فى الاخر

بعد كده بقى هتيجى تحت وتقوله ان المكنة اللى اسمها ns0. دى عبارة عن A يعنى Address وال IP Address بتاعها هو كذا 201.201.0.4

كده الملف بتاعك هيكون بالشكل ده

```
$TTL 1D
@       IN SOA  ns0.ahmed.com. admin.ahmed.com. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      ns0.ahmed.com.
ns0     A       201.201.0.4
```

يبقى كده خليك فاكر ان ال TTL هى ال value اللى انا بحدد على اساسها ال Query دى هيتعملها cache قد اى عند ال Client وهنا عندك فى ال default بيكون لمدةيوم

طيب بص بقى يا برنس ، انت عندك انواع من ال records اول نوع انت شوفته وهو ال NS اللى هو ال Name Server وال NS انت بتستخدمه لما تيجى تعرف DNS Server عندك وده very special record انت بتستخدمه فى حالة واحدة بس ، لما تيجى تعرف DNS Server عندك

فى حاجة تانية لازم تاخد بالك منها وهى انك لما تيجى تعرف Name Server فانت بتعرفه على مرتين اتنين او على خطوتين

الخطوة الاولى بتقوله ان انت عندك Name Server ، والخطوة التانية بتقوله على ال IP بتاعه اللى مربوط بالاسم ده ، كده يعنى

NS ns0.timon.com.

ns0 A 201.201.0.4

من تانى برضو ، دلوقتى انت لما تيجى تعرف DNS اللى هو اسمه برضو Name Server ، فانت بتعرفه على خطوتين ، الخطوة الاولى بتقوله ان انت عندك Name Server Record والخطوة التانية بتقوله على ال IP بتاع ال Record ده اى

طيب على النقيض بقى لو انت عندك عنوان مثلا زى www وال IP بتاعه مثلا 201.201.0.15 بالشكل ده

www A 201.201.0.5

دلوقتى بقى لما تيجى تعرف Address ، محتاج تعرفه فى كام خطوة بقى ؟ هى خطوة واحدة بس

بص بقى بكل بساطة انت فى عندك نوعين من ال records اللى بيتعرفوا فى خطوتين ، اول واحد وهو ال Name Server وده بيتعرف فى خطوتين والتانى وهو ال Mail Server بيتعرف برضو فى خطوتين او بمعنى اخر ال mxrecord بيتعرف فى خطوتين ، واى حاجة تانية بقى بتتعرف فى خطوة واحدة

يبقى كده ال ns record بيتعرف فى خطوتين ، الخطوة الاولى انت بتعلن عنه ، والخطوة التانية انت بتقوله فين ال Actual IP بتاع السيرفر ده او ال Name Server ده بمعنى اخر

طبعا انت دلوقتى بعد ما خلصت الملف ده اطلع بقى منه ، لكن خد بالك من حتة وهى اننا عمالين ننشأ فى ملفات ونحذف فى ملفات وناسيين خالص مين ال Owner بتاع الملفات دى واى ال security context بتاعت الملفات دى واى نظام ال SELinux من الكلام ده كله ،

طيب مبدئيا كده ال owner او ال user اللى هيشغل ال named ك service هو اسمه named ، طبعا لو الملفات بتاعت ال configuration لو مش مملوكة لل user اللى هو named فاكيد طبعا ال service اللى هى named مش هتعرف تقرأ الملفات دى واحتمال متشتغلش

كده انت هتيجى تنفذ الكلام ده

chown root:named ahmed.forward

طيب تانى حاجة وهى علشان تريح دماغك من ال selinux لحد ما نوصل ليها ، فانت هتعمل restore لل context

يبقى انت هتنفذ الامر ده

restorecon -v ahmed.forward

-v =====> verbose

وبعدها بقى تعمل restart لل named–chroot او named على حسب ما انت شغال ، اذا كنت شغال normal named او كنت شغال chrooted named

طبعا لو عايز تتأكد ان ال syntax بتاع ملف ال configuration بتاع named صحيح ، ممكن تنفذ الامر ده

named-checkconf

طبعا لو مظهرلكش اى error يبقى كده الملف ال syntax بتاعه صحيح

تعالى بقى شوف ال status بتاعت named-chroot

systemctl status named-chroot

هتلاقى فى الناتج الجملة دى

Aug 08 17:58:02 server.dns.com named[5269]: zone ahmed.com/IN: loaded serial 0

هنا بيقولك انه عمل load لل zone او للدومين اللى اسمه ahmed.com

وبيقولك كمان ان كل ال zones اتعملها load

Aug 08 17:58:02 server.dns.com named[5269]: all zones loaded

تعالى بقى اسنخدم الاداة اللى dig

dig @201.201.0.4 www.ahmed.com

و dig دى عبارة عن tool بتستخدمها علشان ت Query ال DNS بتاع سيرفر معين ، فانا هنا بقوله انى عايز ا query ال DNS Server اللى ال IP بتاعه 201.201.0.4 وعايز اعمل query على المكنة اللى اسمها www.ahmed.com

يعنى من الاخر كده انا هروح اسأل ال DNS اللى انا عملته اللى ال IP بتاعه 201.201.0.4 هسأله بقى عن تفاصيل المكنة او السيرفر اللى عليه الموقع ده www.ahmed.com

هنا بقى بيقولك one server found

; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62577
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.timon.com. IN A

;; ANSWER SECTION:
www.timon.com. 86400 IN A 201.201.0.5

;; AUTHORITY SECTION:

timon.com. 86400 IN NS ns0.timon.com.

;; ADDITIONAL SECTION:

ns0.timon.com. 86400 IN A 201.201.0.4

;; Query time: 0 msec

;; SERVER: 201.201.0.4#53(201.201.0.4)

;; WHEN: Wed Aug 08 19:14:32 EDT 2018

;; MSG SIZE rcvd: 92

ده بقى ال question بتاعك ، انت هنا سالت على مكنة اسمها

www.ahmed.com وطبعا قصادها خالص بعد حرف ال A مش مكتوب حاجة

لان انت هنا مش عارف العنوان بتاعها اى

;; QUESTION SECTION:

;ns0.timon.com. IN A

طيب لو ملقتش اى Answer ، يبقى فى مشكلة عندك

لكن احنا عندنا الاجابة بالشكل ده

;; ANSWER SECTION:
www.timon.com. 86400 IN A 201.201.0.5

بعد كده بقى عندنا ال authority section ، مين بقى السيرفر اللى هو authoritative او السيرفر اللى هو authorized انه يكون مسؤل عن ال zone دى او الدومين ده اللى هو www.ahmed.com ، اكيد طبعا هو السيرفر اللى اسمه ns0.timon.com

;; AUTHORITY SECTION:
timon.com. 86400 IN NS ns0.timon.com.

فى عندك بقى ال Query دى خدت وقت قد اى

Query time: 0 msec

متنساش تبقى تعمل restart باستمرار لل named-chroot كل ما تعمل اى تغير بسيط جدا فى ملف ال configuration بتاع اى حاجة مرتبطة بيه

اومال اى بقى موضوع ال views ده وال ACL ، متستعجلش هتعرفهم قريب ان شاء الله

كده احنا لحد هنا خلصنا الفديو ده

16-BIND CONT 4

بدأنا فى الفديو رقم 84 ، طبعا احنا المرة اللى فاتت عملنا Zone وكان على ال Master DNS Server ، وروحنا كمان للملف الخاص بال Zone اللى احنا عملناها وكان اسمه ahmed.forward ، وعملنا حاجتين ، اول حاجة اننا اعلنا عن Name Server وبعدها اعلنا عن web server اللى هو كان www لو تفتكر يعنى

وقولنا المرة اللى فاتت ان في شوية Parameters فى الملف ده timon.forward ، هما دول

0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H) ; minimum

او من الاخر كده احنا هنبص على الحاجات دى كلها من تانى

```
$TTL 1D
@       IN SOA  ns0.ahmed.com. admin.ahmed.com. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      ns0.ahmed.com.
ns0     A       201.201.0.4
www     A       201.201.0.5
```

تعالى بقى نبص تانى على الكلام ده كله علشان نعرف اى اللى بيحصل بالظبط فى ال Background وانت شغال

طيب وعلشان تفهم الكلام ده ، لازم اننا نربط ال Master Server بال Slave Server ، يعنى احنا دلوقتى قبل ما هناخد ال reverse Lookup ، تعالى ناخد ال Master Server وال Slave Server ، علشان تقدر تفهم ازاى الاتنين دول شغالين مع بعض

برضو قبل ما نبدأ فى اى حاجة ، فى شوية حاجات كده لازم تاخد بالك منهم ، لو تفتكر المرة اللى فاتت احنا قولنا اننا عندنا حاجتين ، دلوقتى انا اللى موجود عندى حاليا هو ال Master Name Server ، الفكرة بقى كلها قايمة على انى انا لو عندى شبكة كبيرة جدا ، بمعنى ان مثلا لو انا موصل ال Master Name Server على switch والسويتش ده واصل عليه كمية users كتيرة فشخ ، زى انه مثلا ممكن يكون متوصل بالسويتش ده ال Internal Network وواصل بيه كمان ال DMZ وومكن كمان يكون متوصل بيه ال remote users زى مثلا لو عندك VPN Users بيعملوا connect على السويتش ده ، يعنى كمية users كتيرة فشخ ، يعنى مثلا تخيل ان انت عندك شركة والشركة دى فيها 5000 مستخدم وال 5000 دول بيكونوا active كل يوم وليكن مثلا من الساعة 8 لحد الساعة 5 ، وبالتالى الضغط على السيرفر ده هيكون كبير جدا ، فانت هنا بقى عندك حل من اتنين

الحل الاسهل وهو انك تفضل تزود فى ال resources بتاعت السيرفر ده يعنى تزود الرامات والبروسيسور وغيرهم ، بس مهما تزود فى ال resources انت هيكون عندك مشكلة برضو وهى ان ال resources دى مش هتفرق معاك فى حاجة لو السيرفر ده وقع ، بمعنى ان انت لو حبيت تعمل

اى Maintenance Job للسيرفر ده والسيرفر ذات نفسه وقع ، فد فى حد ذاته مشكلة

بمعنى اخر ان لو الهارد وير ذات نفسه بتاع السيرفر وقع فده مشكلة برضو حتى لو المكنة ذات نفسها هنجت فدى برضو مشكلة فى حد ذاتها .

فالحل التانى قالك انت هتعمل سيرفر تانى ، وهنسميه ال Slave Server وهكتب بقى كل ال records على ال Slave Server ده ، يبقى كده الحل بتاع انى ازود ال resources ده مش حل عملى ، يبقى انا كده هعمل مكنة تانية اللى هى ال slave ، والمكنة بتاعت ال Slave دى نفس ال setup بتاعها هيكون هو هو نفس ال Setup بتاع ال Master
لكن كل اللى هعمله انى هقول لل Slave ال Master بتاعه هيكون فين بالظبط واروح بقى لل Master اقوله ان انت عندك Slave فى المكان الفلانى

يبقى كده ال Master هيعرف ال Slave فين وال Slave هيعرف ال Master فين علشان الاتنين يقدروا يكلموا بعض ، طيب حلو ، دلوقتى بقى هل كل ال records اللى انا كتبتها على ال Master ، هل هرجع اكتبها تانى على ال Slave ؟؟ قالك لأ طبعا ، انت فى كل مرة هتعدل فيها على ال Master ، انت هتعدل variable واحد اللى هو ال Serial Number بتاع الملف بتاعك اللى هو عبارة عن رقم Identifier للسيرفر بتاعك ، فانت كل ما تعدل بقى فى ال serial ده ، اوتوماتيك هيروح ال Master يبلغ ال Slave ويقوله خلى بالك انا حصل عندى تحديث ، وخد بقى التحديث ده ، يعنى ال Master هيقول لل Slave ان فى Update حصل فى ال data بتاعت ال File ده

ويبقى انت كده مش هتحتاج تكتب ال records مرة واتنين كل مرة ، انت هتعدل كل حاجة على ال Master وال Slave هياخد ال Update ده اوتوماتيك

طيب تعالى بقى نطبق الكلام ده كله عملى ، بص يا سيدى احنا دلوقتى عندنا اتنين سيرفر ، طبعا واحد فيهم وهو ال Master وده اللى احنا كنا سطبنا عليه ال Package بتاعت ال DNS اللى هى bind و bind-utils و bind-chroot ، تمام كده

دلوقتى بقى هتروح برضو على جهاز ال Slave Server وهتسطب برضو نفس ال Packages دى

yum install bind bind-utils bind-chroot

وبعدها بقى

systemctl disable named

وبعدين

systemctl mask named

وبعدين بقى هنشغل ال service اللى هى named-chroot

/usr/libexec/setup-named-chroot.sh /var/named/chroot on

وبعدها

systemctl enable named-chroot

systemctl start named-chroot

systemctl status named-chroot

طبعا بعد كده انت هتبدأ تعدل فى ملف ال configuration الرئيسى اللى هو named.conf

vim /var/named/chroot/etc/named.conf

وتعدل بقى ال options دى

```
options {
        listen-on port 53 { 127.0.0.1;  };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; };
```

بعد كده بقى هناخد ال Zone اللى احنا عملناها فى ملف ال configuration الرئيسى بتاع ال Master Server اللى هى دى

```
zone "ahmed.com" IN {
        type master;
        file "/var/named/timon.forward";
};
```

ونحطها هى هى فى ملف ال Configuration بتاع ال Slave Server ، لكن بدل ما ال type هيكون master ، لا انا هخليه slave ، وفيه تغيير تانى وهو انى اولا ملف ال record ده

```
file "/var/named/timon.forward";
```

انا مش محتاج اعمله configure على ال Slave Server ، لان هنا ال Slave هو اللى المفروض يروح لل Master ويسحب منه الملف ده

طيب انت اصلا وانت على جهاز ال Slave هتلاقى عندك directory اسمها slaves فى المسار ده

```
[root@client ~]# ls /var/named/chroot/var/named
chroot  data  dynamic  named.ca  named.empty  named.localhost
named.loopback  slaves
```

ال directory دى موجودة علشان كل الداتا اللى هتتنقل من ال Master Server لل Slave Server هتبقى موجودة جواها ، طبعا انت لو جيت دخلت جوه ال directory دى مش هتلاقى جواها حاجة

تعالى بقى ارجع لملف ال named.conf بتاع ال slave ، وهتقوله بقى على ال directory اللى هيتحط فيها الملفات اللى هتتسحب من ال Master Server وكمان اسم الملف اللى هيتسحب هو كمان من ال Master هيكون اى بالظبط يعنى ال Zone بتاعتك فى ملف ال named.conf على جهاز ال Slave Server هتكون بالشكل ده

```
zone "ahmed.com" IN {
        type slave;
        file "/var/named/slaves/timon.forward";
};
```

معنى كده انه المفروض علشان يحصل Zone Transfer ، او بمعنى اخر لما يحصل Zone Transfer ، المفروض ان فى ملف بالاسم ده ahmed.forward هيت create فى المسار ده

/var/named/slaves/

والملف ده بقى الداتا اللى هتكون موجودة جواه ، هتكون متاخدة من ال Master Server

كده كل الشغل اللى على ال Slave خلص ، بس كده انا ناقصنى حاجة واحدة بس ، وهى انى لازم اقول لل master فين ال slaves ، وطبعا لازم اقول لل Slaves فين ال Master يبقى انا كده لازم اعرف كل واحد على التانى

كده انا هروح على ال Master الاول ، واجى عند ال Zone اللى انا عملتها ، واضيف ال Parameter ده

allow-transfere { 192.168.43.76; };

يعنى اقوله مين الجهاز اللى مسموح ليه انه يحصله Zone Transfer ، واكتب بقى ال IP بتاع جهاز ال Slave ، او ممكن اكتب كلمة any برضو

يبقى كده الجهاز ده بس هو اللى مسموح ليه انه يتعمله Zone Transfer طيب دلوقتى بقى عملية ال Zone Transfer ممكن انها تتم بطريقتين

الطريقة الاولى وهى انه كل مرة يحصل تعديل على ال Master يروح مبلغ ال Slave ويقوله ان فى تحديث جديد عنده ويروح ال Master يعمل حاجة كده زى Push او Notify يعنى يبعت ال update اللى عنده لل Slave ، والطريقة التانية ان ال Slave ذات نفسه هو اللى يسأل ال Server يعنى بيعمل Pull يعنى يروح لل Master ويقوله ادينى التحديث اللى عندك
وده بيتم بشكل Periodic على فترات زمنية يعنى ، وده هنبص عليه دلوقتى ، اللى هما الخمسة Parameters اللى اتكلمنا عنهم المرة اللى فاتت او بداية الفديو ده

يبقى كده انت عندك طريقتين علشان تاخد ال records او ال Zone Files من ال Master لل Slave

طيب نرجع بقى لموضوعنا ، احنا دلوقتى فى ملف ال configuration الرئيسى بتاع ال Master اللى هو named.conf ،وكده احنا عرفنا ال Master ان الطرف ده هو اللى مسموح ليه انه يعمل Transfer ، فى برضو عندنا Parameter تانى ، ممكن نعرفه اسمه notify ، وده مع كل مرة انت تعدل فيها رقم الداتا file او بمعنى اخر كل مرة تعدل فيها ال Serial Number عند ال Master ، فال Master هيروح ي Notify ال Slave يقولى خد منى التحديث الجديد ده ، يعنى الشكل بتاعت ال Zone بتاعتك عند ال Master هيكون كده

```
zone "ahmed.com" IN {
        type master;
        file "/var/named/ahmed.forward";
        allow-transfer { 192.168.43.76;  };
        notify yes;
};
```

ال yes دى بقى معناها ، انى كل مرة ك Master يتعدل فيها ال Serial بتاعى هروح ابلغ ال Slave ، ده كده الجزء الاول على جهاز ال Master ، كده معناه انى فعلت ال Push او ال Notify

ناقصلى بقى ال Slave ، لازم اقول لل Slave فين ال Master بتاعك

تعالى بقى على جهاز ال slave ، وعند ال Zone بتاعتك وهتقولى فين ال masters بتوعك ، بالشكل ده

```
zone "ahmed.com" IN {
        type slave;
        file "/var/named/slaves/ahmed.forward";
        masters { 192.168.43.166;  };
};
```

طبعا متنساش تتأكد ان ملفات ال service بتاعت named تكون مملوكة لل user والجروب اللى هما named

كده انت بقى هتروح لملف ال data بتاع ال zone اللى هو فى المسار ده على جهاز ال Master

vim /var/named/chroot/var/named/ahmed.forward

وتقوله ان انت عندك Name Server تانى يعنى عندك DNS تانى ، واسمه مثلا ns1.ahmed.com. وال IP Address بتاعه كذا ، وتكتب بقى ال IP بتاع ال Slave او ايا كان ال IP اللى انت هتكتبه ، علشان مثلا لما تيجى تعمل dig على ال Master DNS وتقوله فين ال IP بتاع الجهاز اللى شايل الموقع اللى اسمه ns1.timon.com. يقولك اتفضل اهو

يعنى خلى بالك مش لازم تكتب ال IP بتاع ال Slave ، اتمنى انك تراجع على النقطة دى كويس فشخ

وبكده الملف بعد التعديل هيكون كده

```
$TTL 1D
@       IN SOA  ns0.ahmed.com. admin.ahmed.com. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      ns0.ahmed.com.
        NS      ns1.ahmed.com.
ns0     A       201.201.0.4
ns1     A       192.168.43.76
www     A       201.201.0.5
```

يبقى انت كده فى ال Zone Files لازم تعرف فين ال Zones بتوعك يعنى فين ال domains بتوعك واى ال IP بتاعتهم ، اوعى تنسى الخطوة دى

بعدها بقى اعمل restart لل named-chroot

systemctl restart named-chroot

وتعالى بقى اعمل

systemctl status named-chroot

هتلاقي فى الناتج سطر بالشكل ده

zone ahmed.com/IN: sending notifies (serial 0)

بيقولك sending notifies ، يعنى بيقولك انه بيحاول يعمل notification دلوقتى او بيحاول انه يبعت notification دلوقتى

تعالى بقى نروح لجهاز ال Slave هو كمان واعمل restart لل named-chroot وشوف بقى بعدها ال status بتاعت named-chroot ، هتلاقى فى الناتج الكام سطر دول

Aug 09 12:48:49 client.dns.com named[3746]: transfer of 'ahmed.com/IN' from 192.168.43.166#53: connected ...8765
Aug 09 12:48:49 client.dns.com named[3746]: zone ahmed.com/IN: transferred serial 0
Aug 09 12:48:49 client.dns.com named[3746]: transfer of 'timon.com/IN' from 192.168.43.166#53: Transfer c...sec)

هنا بقى بيقولك ان قدر يعمل Zone Transfer من السيرفر اللى ال IP بتاعه كذا على البورت واخر سطر بيقولك كمان ان ال Transfer Completed

كده الكلام ده معناه ان الملف اللى هو ahmed.forward اللى موجود على جهاز ال Master Server المفروض انه يكون اتنقل على جهاز ال Slave فى المسار ده

[root@client ~]# ls /var/named/chroot/var/named/slaves/
ahmed.forward

اهو بالفعل الملف اتنقل فعلا لوحده ، بدون ما انا ما اكتبه على جهاز ال Slave من اول وجديد

طبعا الملف ده اللى هو ahmed.forward لو تفتحته على جهاز ال slave هتلاقيه عبارة عن binary file ، وهنا بقى فى حاجة عايز اقولك عليها وهى ان الاصدارات الجديدة فى bind لما بتعمل Zone Transfer ، فالملف اللى انت بتعمله zone transfer ده هيتنقل من جهاز ال Master لجهاز ال Slave على شكل binary file

طيب اى بقى يعم الاشكالية اللى احنا فيها دى ، بص الملف لما بيتنقل بالشكل ده اللى هو بيكون binary file ، بيديك ميزة صغيرة جدا
اول حاجة وهى ان عملية ال Zone Transfer بتكون سريعة جدا ، فانت مثلا لو بتتكلم على Production Environment وعندك Zones 100 ، فانت كده بتجهد ال service دى
فانت بدل ما تقعد تعذب نفسك ، الافضل انك تسيب ملفات ال Zones دى تتنقل بشكل binary زى ماهى ، والحل التانى وهو اذا كنت انت عايز تشوفه ك Plain Text فانت هتقول لل Master وانت بتعمل Zone Transfer ده ابقى اعمله Plain Text

طب اى بقى الحل الافضل ؟؟ طيب بص عندك كده فى سيناريو ممكن يخليك تشد فى شعرك ، انت دلوقتى عندك ال Master شغال زى الفل وال Slave برضو شغال زى الفل وعملية ال Zone Transfer شغالة ومفيهاش مشكلة

وهوب بقى المكنة اللى عليها ال Master Server هنجت ووقفت خالص لاى سبب بقى ، زى مثلا ممكن يحصل Failure فى الهاردوير عندك

فانت بقى علشان تريح نفسك ، اولا خلى فى بالك ان ال DNS او bind عموما ، لما بيعمل ال Zone Transfer ، بيعملوا Load فى ال Memory ، ومعنى كده ان عملية القراءة والكتابة بتكون سريعة جدا ، وعادة يعنى فى معظم ال Environments بيكون عندك اقل من Zone 100 ، طيب انت ليه بقى تحط نفسك فى ال risk ؟

وبالتالى الحل الافضل هنا اننا خليها Plain Text علشان لو ال Master وقع تقدر انت وانت على جهاز ال Slave تاخد ال Zones دى Copy وتبدأ بقى انك تعمل rebuild لل Master من اول وجديد بكل سهولة

كده انت هتيجى على جهاز ال Slave Server ، وتعدل فى ملف ال named.conf وتضيف ال Parameter ده

vim /var/named/chroot/etc/named.conf

```
options {
        listen-on port 53 { 127.0.0.1; 192.168.43.76;  };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; 192.168.43.0/24; };
        allow-query-cache       {localhost; 192.168.43.0/24; };
        masterfile-format text;
```

يعنى انت هنا بتقوله ان ال format بتاعك اللى هياجى من ال Master خليهولى Plain Text

masterfile-format text;

وبعدها بقى اعمل restart لل named-chroot وانت على جهاز ال Slave كل ده

systemctl restart named-chroot

وبعدها بقى روح شوف الملف اللى اتنقل من عند ال master هل بقى Plain text ولا زى ما هو binary

cat /var/named/chroot/var/named/slaves/ahmed.forward

هتلاقيه انه بقى Plain Text والحمد لله

طيب فى حاجة تانية عايز اقولك عليها وهى انى وانا على جهاز ال Master لو انا بقى عدلت حاجة ، هل بقى لازم اعدل برضو عند ال Slave ؟ اكيد طبعا لأ

لما تيجى تعدل بعد كده ، كل التعديل اللى هتعمله هيكون من عند ال Master نفسه
يعنى مثلا تعالى على جهاز ال Master وليكن مثلا اننا عايزين نضيف record جديد فى ملف ال zones بتاعنا

vim /var/named/chroot/var/named/ahmed.forward

يعنى مثلا ممكن يكون عندى record جديد اسمه mail و mail ده بقى هو عبارى عن subdoamin من ال Name Server اللى هو timon.com بس mail ده موجود على سيرفر ال IP بتاعه كذا

فانا بقى هضيفه بالشكل ده ، ومتنساش تغير ال serial بدل ما هى ب zero خليها بواحد

```
$TTL 1D
@       IN SOA  ns0.ahmed.com. admin.ahmed.com. (
                                        1       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      ns0.ahmed.com.
        NS      ns1.ahmed.com.
ns0     A       201.201.0.4
ns1     A       192.168.43.76
www     A       201.201.0.5
mail    A       192.168.43.165
```

وبعدها بقى هتعمل restart لل named-chroot

روح بقى على جهاز ال slave ، وشوف كد الملف بتاع ال Zones هتلاقي ان التحديث اللى حصل على ال master اوتوماتيك اتنقل لل slave

cat /var/named/chroot/var/named/slaves/ahmed.forward

```
[root@client ~]# cat /var/named/chroot/var/named/slaves/ahmed.forward
$ORIGIN .
$TTL 86400      ; 1 day
ahmed.com               IN SOA     ns0.ahmed.com. admin.ahmed.com. (
                                   1          ; serial
                                   86400      ; refresh (1 day)
                                   3600       ; retry (1 hour)
                                   604800     ; expire (1 week)
                                   10800      ; minimum (3 hours)
                                   )
                        NS     ns0.ahmed.com.
                        NS     ns1.ahmed.com.
$ORIGIN ahmed.com.
mail                    A      201.201.0.8
ns0                     A      201.201.0.4
ns1                     A      192.168.43.76
www                     A      201.201.0.5
```

طيب ولو ملقتش ان الملف ده اتعدل ، يبقى جرب تمسحه وانت على ال Slave وتعمل restart لل named-chroot على جهاز ال Slave برضو

دلوقتى بقى ال best practice ليك ، لو انت بتتكلم على Enterprise Network كبيرة ، وعندك مثلا بتاع 3000 مستخدم ، فانت المفروض عندك لما تستخدم ال DHCP ، انت طبعا بتقوله ال range بتاعك هيكون من فين لفين بالظبط ، وعلشان بقى توزع ال Load على السيرفرين دول ، هتعمل اى بقى ، هتروح انت عند ال configuration بتاع ال DHCP وتروح تقول لل range الاول من الايبهات ان ال Master Server بتاعكم هو السيرفر رقم واحد وال slave server هو السيرفر رقم 2 ، وتيجى لل range التانى العكس يعنى ال Master Server هو السيرفر رقم 2 وال Slave Server هو السيرفر رقم 1 وبكده انت ضمنت ان ال Load هيتوزع على الاتنين ، وبكده انت مش محتاج اى High Availability او حتى اى Extra Tools تشغلها

طيب فى حاجة تانية عايز اقولك عليها ، وهى افرض ان انا عندى Client مثلا وال Client ده عايز resolve موقع google.com ، طبعا ال client هيبص على ال configuration اللى عنده هيشوف مين ال master dns يعنى مين ال DNS الاساسى بتاعك اللى هو مثلا ممكن يكون 8.8.8.8 وال slave dns ممكن يكون مثلا 8.8.4.4

يبقى كده جهاز ال Client هيبعت ال request لل DNS الاول ، وطبعا لو ال DNS الاول ده مش reachable يبقى اكيد هيتنقل للتانى ، وهكذا بقى

طبعا ال client زى ما انت عارف لما بيعمل communicate مع السيرفر بيعمل communicate على بورت 53 UDP

انما بقى لما السيرفر بي communicate مع السيرفر التانى علشان يعمل عملية ال Zone Transfer بي communicate على بورت 53 بس TCP ، فطبعا لو انت عامل enable لل firewall على اى مكنة فيهم ، فانت لازم تسمح بالبورت ده ، وخلى بالك ان الكاش بتاع ال DNS مش بيتنقل ، لان الطبيعى بتاع الكاش انه بيكون فى ال memory

تعالى بقى ننقل على حاجة تانية ، دلوقتى بقى انا عندى ال Master Server موجود وال Slave Server I موجود والاتنين شغالين تمام ، طيب احنا اصلا عرفنا اننا عندنا Parameter اسمه serial ، وده كل وظيفته انه لو حصل اى تحديث على ال Master ، فيبدأ بقى ال Master يبلغ ال Slave انه فى تحديث حصل ، فكده ال slave بيقارن ال serial اللى عنده بال serial اللى عند ال Master ويشوف اى التغييرات اللى حصلت ، وبيقولك بقى انه عادة الناس بيحاول انهم يخلوا ال value بتاعت ال serial number تكون مكافأة لليوم بتاعك ، يعنى مثلا لو احنا النهارده فى 2018 واحنا فى شهر 8 والنهارده يوم 10 يعنى ال serial بتاعك بيكون كده

20180810 serial;

يعنى ال serial هو عبارة عن السنة والشهر واليوم ، وفى ناس كده بتحب تضيف filed تانى وتحط الساعة والدقيقة ، بس موضوع انك تحط الساعة والدقيقة ده مش شئ كويس او ملوش لازمة، لان انت غالبا يعنى مش كل ساعة هتروح تعدل فى ملف ال data بتاع ال bind ، وده طبعا لا يمنعك انك تستخدم اى رقم

طيب كده ال serial وعرفناه ، اومال بقى اى بقية ال Parameters دى

1D ; refresh
1H ; retry
1W ; expire
3H) ; minimum

ببساطة شديدة لو روحت لجهاز ال slave وشوفت الملف ده

cat /var/named/chroot/var/named/slaves/timon.forward

هتلاقى ال Parameters دى بالتفصيل اهى

86400 ; refresh (1 day)
3600 ; retry (1 hour)
604800 ; expire (1 week)
10800 ; minimum (3 hours)

طيب احنا قولنا ان فى ال Serial ، ال Master ذات نفسه هو اللى هيروح ي notify ال slave بال update اللى حصل عنده ، انما بقى فى ال Parameters التانية هيروح ال slave من نفسه كده يسأل ال Master والفترة دى بقى بتتحدد بناءا على ال refresh value ، هنا مثلا ال value بتاعت ال refresh كل يوم
يبقى كده ال refresh هو الوقت اللى Slave Server هيستناه قبل ما يروح يسأل ال Master Server اى التحديث اللى عندك

بعد كده بقى ال retry ، هنا بقى افرض ان ال Slave Server لما راح يسأل ال Master Server لقى ان ال master مش شغال او down ، فهو هنا بقى هيعمل retry بعد قد اى بقى ؟
طبعا هيعمل retry بعد يوم زى ما متحدد عندنا هنا

انما بقى ال expire هو الوقت اللى انا ها declare ان كل ال data files او ال Zones اللى كانت متاخدة من ال Master بقت خلاص expired عند ال slave server وليكن فرضا بعد اسبوع واحد

اخر Parameter عندنا وهو ال minimum ، وده معناه مثلا ان لو مثلا حد جه وسأل ال DNS على record وليكن مثلا www.yahoo.com فيروح ال DNS يرد عليه ويقوله ان ال IP Address بتاع ال record ده او الموقع ده هو كذا 165.684.18.8 ويروح ال DNS يقوله بص يعم ، خلى الناتج ده فى الكاش عندك لمدة 3 ساعات مثلا
طيب كده ال DNS بيقول للى بيسأله انه على الاقل ميسألش تانى الا بعد 3 ساعات ، طب اومال بقى على الاكتر هى اى بقى ؟
على الاكتر بقى هى ال value بتاعت ال Time To Live

$TTL 86400; 1 day

كده احنا خلصنا ان ال DNS بتاعنا بيشتغل ك Forward Lookup وبقى عندنا كمان Slave Server بيعمل Zone Transfer

المرة القادمة ان شاء الله هنتكلم على ال reverse lookup بالاضافة لل views وال ACL وبالاضافة برضو انى هقول ان السيرفر اللى عليه ال key الفلانى ده هو ده بس اللى مسموح ليه بعملية ال Zone Transfer

17-BIND CONT 5

ده اخر فديو فى موضوع ال DNS ، النهارده بقى عندنا موضوعين مهمين جدا ، الموضوع الاول وهو ازاى انك ت Implement ال DNS Views والموضوع التانى وهو ازاى انك ت Implement ال Transaction Signature او زى ما بنسميها ال KSIG

تعالى بقى نتكلم على ال DNS Views ، طبعا احنا المرة اللى فاتت كان عندنا اتنين سيرفر ، واحد اللى هو ال Master DNS والتانى هو ال Slave DNS وكنت على ال Master Server كنا بنحدد عليه ال Zones وكنا بنقوله اننا مثلا عندنا Zone اسمها ahmed.com وعندى برضو شوية hosts او شوية subdomain جوه ال zone دى زى مثلا www.ahmed.com

وبعد كده بقى روحنا عملنا ال Slave Server ونقلنا كل ال Zones من على ال Master Server ووديناها لل Slave ، بمعنى اصح انى مكنتش محتاج اكتب كل ال records او ال Zones دى من تانى ، ده كل اللى احنا عملناه وكان مجرد حاجة بسيطة جدا وبدائية كمان

اى بقى اللى احنا عايزين نعمله النهارده ؟ بص تعالى بقى نصعب الدنيا شوية ونتعامل مع real world scaniros ، دلوقتى لو انت شغال فى شركة ، فانت بتفصل الشبكة بتاعتك لجزئين وممكن 3 اجزاء كمان واحيانا اكتر من كده كمان ، ازاى بقى ؟؟ بص يا سيدى انت دلوقتى الشبكة عندك بتكون مقسمة لاجزاء ، مثلا بيكون عندك ال DMZ وال Internal Network وهكذا بقى ، فانا مثلا بكون محتاج اعزل او انى اعمل اكتر من view عندى ، بحيث ان ال user لو جى من بره الشبكة بتاعتى يكون ليه Access على ال subdoamin ده بس

www.ahmed.com

و

mail.ahmed.com

فانت بقى الشبكة بتاعتك ، بتكون واصلة بجزبين ، اول جزء وهو ال Guest Network والجزء التانى وهو ال Local Network ، طبعا فى الواقع الدنيا بتكون اعقد من كده بس ده مجرد سيناريو مبسط

فانت بكل بساطة عايز الناس اللى هما جايين عن طريق ال Public Net وليس عن طريق ال Guest Network ولا ال Local Network ، انت بقى عايز الناس اللى جايين من بره خالص دول يبصوا بس على ال 2 hosts دول

اللى هما www و mail ، فانت مثلا عايز ت configure ال DNS وتقوله ان انت عايز تعمل 3 View

تقوله بقى ان ال View الاولى لو الراجل جاى عن طريق ال Internal Network فانت هتوريله كل ال Hosts اللى عندى ، سواء بقى كانت www او mail او حتى data base

وال View التانية او ال rule التانية ان لو الراجل جاى عن طريق ال Guest Network فانت يا DNS هتوريله ال www ووريله كمان ال Portal بتاعك ووريله كمان ال Guest Video Confrense وكمان ال Access بتاع ال Projector ، طبعا متنساش ان كل device بيكون ليها اسم وليها IP

وال View التالتة بقى لو اى حاجة غير اللى فاتوا فانت هتورى الراجل اللى جى عن طريق ال Public Network هتوريله ال www وال mail

ده بقى كله باختصار شديد اللى احنا عايزين نعمله دلوقتى ، بالمناسبة ال Views بيسموها كده Split View DNS او Split Horizon ، فكده الراجل اللى جى من بره هيشوف records معينة ، والراجل اللى جى من ال Guest او من ال Internal Network هيشوف Records تانية خالص

يعنى الفكرة كلها ، فى ان الراجل اللى جى من ال Public Network هيكتب فى ال browser عنده www.ahmed.com او مثلا mail.ahmed.com بس ، وهيروح لجهاز ليه IP مختلف ، لان ده اللى متحددله بس ، اما بقى لو هو داخل ال Internal Network وكتب فى المتصفح بتاعه www.ahmed.com فهو هيروح لجهاز تانى خالص وليه IP تانى خالص ، غير الجهاز اللى هيوصل ليه الشخص اللى جى من ال Public Network

يعنى الاتنين بيكتبوا نفس الاسم اللى هو www.ahmed.com وبيروحوا لنفس ال DNS Server اللى عندك فى الشركة ، بس اللى جى من ال Public Net هيروح لمكنة ، واللى جى من ال Internal Network هيروح لمكنة تانية خالص

طبعا مع الاخذ فى الاعتبار ان مفيش حد يقدر يمنعك انك تقدر انك تبعت الاتنين على نفس المكنة ، بس طبعا انت كده خسرت ال function بتاعت ال DNS لان عادة ال Split View DNS انت بتعملها علشان تعزل المستخدمين عن بعض

بالنسبة بقى لل Implementation ، او التطبيق يعنى ، فهو سهل جدا هنروح بقى على جهاز ال Master Server ، وهنفتح ملف ال named.conf

vim /var/named/chroot/etc/named.conf

طبعا احنا كنا معرفين فيه zone اسمها ahmed.com ، وكمان قولته على المكان اللى هيكون فيه الملف اللى هيكون فيه ال record بتاعتى او الداتا بمعنى اخر

file "/var/named/ahmed.forward";

تعالى بقى نعرف ال views بتاعتنا ، هتقولى وهو انا هحفظ ال configuration بيتكتب ازاى كمان ؟ هقولك طبعا لأ مفيش عندنا حاجة اسمها حفظ

انت هتلاقي عندك اصلا sample file موجود فى المسار ده

/usr/share/doc/bind-9.9.4/sample/etc/named.conf

روح بقى خد من ملف ال sample ده ال configuration اللى انت عايزه ، واعمله Paste فى المكان اللى انت عايزه برضو

```
view "localhost_resolver"
{
/* This view sets up named to be a localhost resolver ( caching only
nameserver ).
 * If all you want is a caching-only nameserver, then you need only define
this view:
 */
        match-clients           { localhost; };
        recursion yes;
```

```
        # all views must contain the root hints zone:
        zone "." IN {
                type hint;
                file "/var/named/named.ca";
        };

        /* these are zones that contain definitions for all the localhost
         * names and addresses, as recommended in RFC1912 - these
names should
         * not leak to the other nameservers:
         */
        include "/etc/named.rfc1912.zones";
};
```

روح بقى الزقه فى ملف ال configuration الرئيسى بتاع ال Master Server

تعالى بقى سيب الملف ده دلوقتى ، وهنشرح شوية حاجات كده ، اولا مع ال BIND لما تيجى تعمله implementation فانت عندك حل من اتنين ، الاول وهو انك تعرف ال BIND بتاعك ده with Views ، او يا اما without views ومينفعش تعمل mix ، بكل بساطة اللى احنا كتبناه ده معناه ان انت لو جيت مثلا فى ملف ال named.conf وكان عندك zone وجيت عرفت view واحدة فانت مينفعش تيجى فى جزء تانى من الملف وتيجى تعرف zone وتسيبها عريانة متكونش جوه اى view

الكلام من تانى ، مينفعش تروح عامل Zone وتحطها فى View وبعدين تروح تعمل zone تانية ومتحطهاش فى view ، الكلام ده عك ، لان انت اصلا لما تيجى ت restart ال service هيطلعلك errors ، فانت بقى لو معملتش views خالص يبقى خلاص خير وبركة ، انما بقى لو حطيت zone فى view يبقى لازم تحط الباقيين فى view برضو

دى كده اول حاجة اتفقنا عليها

الحاجة التانية بقى ، انت فى ملف ال configuration عندك كان فيه section فى الاول خالص اسمه options ، وكنت بتحط فيه كل ال options بتاعتك ، دلوقتى بقى ايا كان ال option اللى انت حطيته فوق ، اى بقى option انت هتحطه فى ال view فهو هي overwrite ال global option واظن انت عارف حاجة زى دى

تعالى بقى نرجع لملف ال named.conf ، دلوقتى بقى هسمى ال view بتاعتى مثلا باسم Internal ، بعد كده بقى ال view دى هت match انهى clients بالظبط
فانا مثلا ممكن اقوله ان ال view دى هت Match ال clients اللى جاييين من الشبكة اللى هى 201.201.0.1/24 ومتنساش ال ; وكمان المسافة اللى فى الاخر

يبقى كده اى client هياجى من ال source ده هيعمله match يعنى هيسمحله

خلى بالك ان انت عندك ال Zone اللى انت كنت عاملها المرة اللى فاتت اللى هى ahmed.com ، فانت بقى هتخليها جوه ال view اللى انت بتعملها دى

اه بالمناسبة فاكر ال Zone "." دى ، طب فاكر الملف بتاعها اللى هو

vim /var/named/chroot/var/named/named.ca

الملف ده بقى يا برنس ، فيه معلومات ال root servers كلهم

حط بقى فى اعتبارك وخد القاعدة التالتة بالنسبة لل Views ، وهى ان اى view هتعملها لازم يكون فيها definition لل zone بتاعت ال root servers حتى لو عندك 500 view والا بقى لو ال Zone دى اللى هى ahmed.com متعرفش توصل لل root servers فال DNS مش هيعرف يعمل resolve اصلا

يعنى مثلا انت لو عملت match لل clients اللى جاية من ال Network اللى هى 201.201.0.1 ما كده كده ال Clients دول لازم يكونوا عارفين ال root servers ، والا فانت ال DNS بتاعك مش هيعرف يعمل resolving علشان كده كل view لازم يكون فيها definition لل zone بتاعت ال root server

نرجع بقى للملف بتاعتنا ، دلوقتى انت كان عندك فى الملف ال zone دى لوحدها

```
zone "." IN {
        type hint;
        file "named.ca";
};
```

فانت هتمسحها بقى ، لان انت اصلا معرفها جوه ال view اللى انت هتعملها

يبقى انت كده الشكل النهائى بتاع ال view بتاعتك اللى اسمها internal هيكون كده

```
view "internal"
{
        match-clients           { localhost; 201.201.0.1/24;  };
        recursion yes;

        # all views must contain the root hints zone:
        zone "." IN {
                type hint;
                file "/var/named/named.ca";
```

```
        };

        /* these are zones that contain definitions for all the localhost
         * names and addresses, as recommended in RFC1912 - these
names should
         * not leak to the other nameservers:
         */
        include "/etc/named.rfc1912.zones";

zone "timon.com" IN {
        type master;
        file "/var/named/ahmed.forward";
        allow-transfer { 192.168.43.76;  };
        notify yes;
};

};
```

ولو موضوع كتابة ال Zone اللى هى ال . dot الخاصة بال root servers ، لو موضوع كتابتها كل شوية متعب بالنسبالك ، فانت ممكن تعمل ملف خارجى وليكن مثلا

vim named.roots

وتحط جواه ال zone دى

```
 zone "." IN {
                type hint;
                file "/var/named/named.ca";
        };
```

وبعدها بقى تعمله include فى اى view انت هتعملها ، وبكده انت ممكن تكون وفرت على نفسك

الحاجة التانية اللى البشمهندس بيحب يعملها وهى متعلقة بجزء ال logging طبعا هو اتكلم عن موضوع ال logging ده وازاى نعمل enable لل logging ، بيتكلم برضو انه جزء ال logging ممكن ان انت تحطه فى ملف لوحده وتعمله include برضو ، ابقى راجع برضو موضوع ال logging ده برضو

المهم بقى ، دلوقتى اعمل restart لل named-chroot

systemctl restart named-chroot

هتلاقيه بيقولك error ، وبيقولك ان الملف اللى هو

/etc/named.rfc1912.zones

لازم انك تعمل comment للسطر ده

include "/etc/named.rfc1912.zones";

لانه global ، ولانه موجود منه نسخة فى ال view اللى انت عملتها

وبعدها بقى اعمل restart لل named-chroot ، هتلاقيها اشتغلت معاك ، بس موضوع تغيير ال IP ده مش اساسى يعنى ، الفكرة كلها كانت فى السطر ده اللى هو متكرر

طيب علشان بقى تتاكد ان عملية ال resolving شغالة كويس ، استخدم dig

dig @201.201.0.5 www.ahmed.com

هتلاقيها شغالة كويس وزى الفل

تعالى بقى نعمل view تانية ونشوف ازاى هنعمل manipulation للمعلومات اللى طلعتلنا من استخدام dig

افتح تانى ملف ال named.conf على جهاز ال Master

vim /var/named/chroot/etc/named.conf

هنعمل بقى view تانية ونسميها external مثلا ، وهيكون فيها مثلا نفس المعلومات ، بس المرة دى هغير اسم الملف ده

file "/var/named/external-ahmed.forward"

هضيفله بس كلمة external

وبعدين بقى هروح للمسار ده

cd /var/named/chroot/var/named/

وبعدها بقى هتعمل نسخة من نفس الملف السابق اللى هو ده ahmed.forward بس هتسميه بالاسم ده external-ahmed.forward

cp timon.forward external-ahmed.com

وافتح بقى الملف ده

vim external-ahmed.com

وغير مثلا ال IP Address بتاع www وخليه مثلا 184.44.18.49 اى IP وخلاص

وبعدين بقى احفظ الكلام ده

يعنى ال view بتاعتك الشكل النهائى ليها هيكون كده

```
view "external"
{
	match-clients		{  201.201.0.1/24;  };
	recursion yes;

	# all views must contain the root hints zone:
	zone "." IN {
		type hint;
		file "/var/named/named.ca";
	};

	/* these are zones that contain definitions for all the localhost
	 * names and addresses, as recommended in RFC1912 - these
names should
	 * not leak to the other nameservers:
	 */
	include "/etc/named.rfc1912.zones";

zone "timon.com" IN {
	type master;
	file "/var/named/external-timon.forward";
	allow-transfer { 201.201.0.2;  };
	notify yes;
};

};
```

وبعدها بقى اعمل restart لل named-chroot ، وجرب بقى بعدها انك تعمل dig هتلاقيه انه بيسمح لل clients اللى انت حددتهاله

فى معلومة تانية وهى ان ال bind dns بي support حاجة اسمها ال GeoIP Data Base ، ودى عبارة عن data base كبيرة حوالين العالم فيها معلومات كل مدينة فى كل دولة

هتسال طب انا هستفيد من كده اى ؟؟ هستفيد انى ممكن اقول لل DNS بتاعى ان لو ال user جى من دولة زى مصر مثلا فانت هتوريله hosts معينة بايبهات معينة

ولو مثلا جى من مدينة تانية او دولة تانية وريه hosts تانية ، معنى كده انى ممكن اعمل matching بناءا على ال city اللى ال user جى منها

فانت مثلا ممكن تيجى فى ال view بتاعتك وتحددل ل dns هو هي match انهى مدينة بالظبط بناءا على الايبهات

ممكن تروح لل man page بتاعت named.conf عن طريق

man 5 named.conf

من الحاجات المهمة جدا جدا برضو وانت شغال مع ال named ، ان انت لازم تخبى ال version number بتاعت ال named ، لان ال DNS واحد من اهم ال Infrastructure services الموجودة

بمعنى ادق ان لو ال bind حصله hack فانت كده بقيت فى السلامة ، روحت فى ابونكلة زى ما تيمون بيقول 😂😂😂

فانت بقى ممكن تغير ال version بتاعت ال named او bind يعنى ، وعلشان تغير ال version فانت ممكن تقوله فى section ال options ال parameter ده

version "za3bola DNS"

بالشكل ده

```
options {
        listen-on port 53 { 127.0.0.1; 201.201.0.1;  };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; 192.168.43.0/24; };
        allow-query-cache       {localhost; 192.168.43.0/24; };
        version "za3bola dns";
```

وبكده اى حد هيحاول انه ي attack على vulnerability معينة ، فهيشوف ال version مختلف تماما

وبعدها بقى اعمل restart لل named-chroot

تعالى بقى دلوقتى ممكن تستخدم dig علشان تتأكده ان ال version بتاعت ال bind بقت za3bola زى ما انت ما سميتها

dig @201.201.0.5 -c CH -t txt version.bind

-c ======== for class

-t ======== for text

هتلاقى الناتج بالشكل ده

```
;version.bind.                  CH    TXT

;; ANSWER SECTION:
version.bind.           0       CH    TXT   "za3bola dns"

;; AUTHORITY SECTION:
version.bind.           0       CH    NS    version.bind.
```

وبالتالى انت لازم لازم انك تخبى ال version بتاعك بتاع ال bind ، وده من ضمن اساسيات ال security

عارف مثلا انت لو جيت تشوف ال version بتاع google هتلاقيه مخبى هو كمان ال version

dig @8.8.8.8 -c CH -t txt version.bind

ان شاء بكره هنتكلم على ال TSIG اللى هى ال Transaction Signature ، وازاى نعمل zone transfer مع ال TSIG اللى هى تقريبا ناس من ال system admins بيقولوا عليها انها رخمة

ليه بقى ؟؟ تعالى بقى نوضح الدنيا

دلوقتى انا عندى master server وعندى كمان slave server ، وعندى على ال master server عندى view اسمها internal وفيها zone اسمها ahmed.com وعندى برضو على ال Master Server عندى view تانية اسمها external وفيها zone تانية اسمها برضو ahmed.com

دلوقتى بقى انا لما اجى اقول لل Slave Server اللى عندى لما اجى اقوله انى عايز اعمل zone transfer من ال Master من ال zone اللى اسمها timon.com ، فهو بقى هي match انهى واحدة فيهم ؟ يعنى هي match اللى هى موجودة فى ال view اللى اسمها internal ولا ال view التانية اللى اسمها external ، كده انت لبست يا برنس

فاحنا بقى المرة الجاية ان شاء الله هناخد ال TSIG ، وازاى استخدم ال TSIG فى انها تفرقلى بين ال zone اللى موجودة فى ال view الاولى وبين ال zone اللى موجودة فى ال view التانية ، ودى واحدة من اكبر المواضيع بتاعت ال DNS اللى الناس بتهرب منها

لحد هنا وكده احنا خلصنا معظم ال **Basics** بتاعت ال **DNS**

متنساش بقى تراجع الملاحظات اللى موجودة فى الصفحة رقم 4 و 5 و 6

انتهى الجزء الثالث