الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة ابن خلدون - تيارت
كلية الرياضيات والاعلام الالي
قسم : الإعلام الآلي

مذكرة مقدمة لاستكمال متطلبات شهادة الماستر
لكية الرياضيات والاعلام الالي
تخصص : شبكات واتصالات سلكية ولا سلكية

من اعداد :

- **بصديق نرجس**
- **جيلالي حياة الهام**

تحت عنوان:

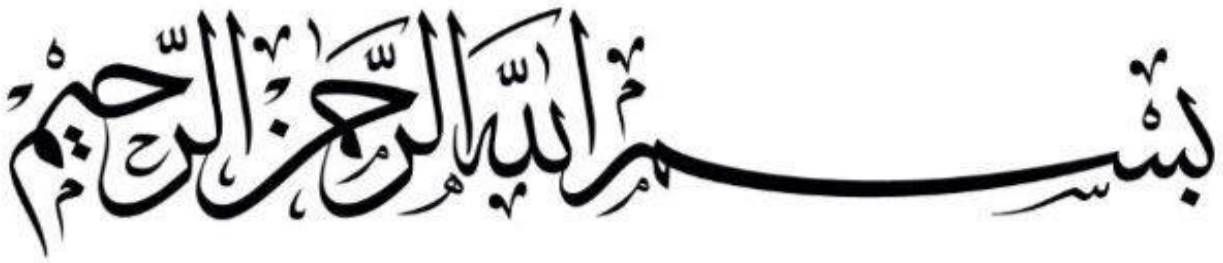
تركيب أداة للمراقبة والرصد للشبكة باستخدام برنامج حر

MISE EN PLACE D'UN OUTIL DE MONITORING DE RESEAU A BASE DE LOGICIEL LIBRE

نوقشت علنا أمام اللجنة المكونة من :

دحماني يوسف	**الرتبة أستاذ**	**المشرف**
مصطفاوي سيداحمد مختار	**الرتبة أستاذ محاضر" A"**	**الرئيس**
عالم عبد القادر	**الرتبة أستاذ مساعد"A"**	**المناقش**

السنة الجامعية: 2023/2022


بسم الله الرحمن الرحيم

شكر وعرفان

بسم الله الرحمن الرحيم

كما نتوجه بالشكر الجزيل إلى من شرفنا بإشرافه على مذكرة بحثنا الأستاذ الدكتور " **دحماني يوسف**"الذي لن تكفي حروف هذه المذكرة لإيفائه حقه بصبره الكبير علينا، ولتوجيهاته العلمية التي لا تقدر بثمن؛ و التي ساهمت بشكل كبير في إتمام و إستكمال هذا العمل؛

الى الاستاذ الدكتور **"مبارك داود "**.عندما أتذكر كل ما قدمته لي خلال مشوار دراستي، يقف لساني عاجزاً عن القول فلا توجد كلمات شكر أو عبارات تقدير توفي لك حقك، فكنت بمثابة الاخ و المحفز الرئيسي والداعم الأول لي خلال مشوار دراستي

إلى كل أساتذة قسم **"الرياضيات والإعلام الى "** عامة والى اساتذة تخصص **"شبكات واتصالات سلكية ولا سلكية "** خاصة كل باسمه لكم منا الف شكر وتحية .

حياة و نرجس

عن رسول الله صلى الله عليه و سلم قـال:

" من لم يشكر الناس لم يشكر الله "

الحمد الله على إحسانه و الشكر له على توفيقه و امتنانه و نشهد أن لا إله إلا الله وحده لا شريك له تعظيما لشأنه و نشهد أن سيدنا و نبينا محمد عبده و رسوله الداعي إلى رضوانه صلى الله عليه و على آله و أصحابه و أتباعه و سلم .

بعد شكر الله سبحانه و تعالى على توفيقه لنا لإتمام هذا البحث المتواضع أتقدم بجزيل الشكر إلى الوالدين العزيزين **"أمي"**و **"أبي"** الذين أعانوني و شجعوني على الاستمرار في مسيرة العلم و النجاح،و إكمال الدراسة الجامعية و البحث وعلى صبرهم معي في كل عثرة حياة

و إلي الوالدين العزيزين الذين منحوا لي اسما ثانيا **"قرني"**

إلى كل من إخوتي : **"احمد ،علي، محمد** " شكرا لكم

إلى كل من أخواتي : **"ناجية و أمينة ومسعودة ونور الهدى** " أحبكم

إلي زوجي العزيز وتاج رأسي **"نور الدين"** وقرة عيناي ابني وابنتي **"عبد الصبور"** و **"نورهان** " إليكم اهديه

إلي كل من يدرس معي " **2MRT**" أجمل الأصدقاء **"حياة ،أمال ،عائشة ،خليدة ،إسماعيل ،نبيل، هارون** " كل باسمه أشكركم على كل الدعم لولاكم لما وصلت اليوم

ومن يعمل معي لكم مني ألف شكر علي دعمكم

كما أتوجه بخالص شكري و تقديري إلى كل من ساعدني من قريب أو من بعيد على إنجاز و إتمام هذا العمل .

"رب أوزعني أن أشكر نعمتك التي أنعمت علي و على والدي و أن أعمل صالحاً ترضاه و أدخلني برحمتك في عبادك الصالحين"

نرجس

بسم الله الرحمن الرحيم

«وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ ...»(التوبة – 105)

اله لا يطيب الليل إلا بشكرك ولا يطيب النهار إلا بطاعتك ... ولا تطيب اللحظات إلا بذكرك ...

الحمد لله الذي وفقني لتثمين هذه الخطوة في مسيرتي الجامعية بمذكرتي هذه ثمرة الجهد والنجاح وحصاد تعب السنوات ، لم تكن الرحلة قصيرة ولا ينبغي لها أن تكون ، لم يكن الحلم قريبا ولا الطريق كان محفوفا بالتسهيلات لكنني فعلتها .

أهدي ثمرة جهدي هذا إلى :

إلى من رباني وكافح من أجلي ... إلى المصباح الذي أنار دربي ... أرجو من الله أن يمد في عمرك لترى ثمارا قد حان قطافها بعد طول انتظار ... أبي الغالي .

إلى تلك الإنسانة العظيمة التي طالما تمنت أن تقر عينها برؤيتي في يوم كهذا ... إلى من كانت خطاي كفيفة دون نور كفيها إلى نعمتي و جنة قلبي "أمي الحبيبة " .

إلى صاحب الفضل عمي العزيز "الجيلالي" الذي كان له بالغ الأثر في إزالة الكثير من العقبات والصعاب فكان ظلي حين يصيبني التعب ورفيقي في هذا النجاح وقرة عين لي في هذه الحياة .

إلى من شددت عضدي بهم وكانوا لي ينابيع وكنت من كل ينبوع أستقي لأرتقي إخوتي الأعزاء(محمد ، بسملة ، ملاك ، سيرين) .

إلى صديقات الأيام ،إلى من كانتا في الأيام العجاف سحابا ممطرا صديقاتي "فضيلة و نرجس" .

والى أولئك الذين يفرحهم نجاحنا ويحزنهم فشلنا إلى الأقارب و الأصدقاء قلبا ودما و وفاءا الذين مهدوا عثرات مسيرتي بدعائهم وأنسوني صعابها بحبهم .

كما أهدي ثمرة جهدي لأستاذي الفاضل الدكتور:"دحماني يوسف" الذي كلما تظلمت طرق العلم أمامنا لجأنا إليه فأنارها لنا و الذي كلما سألناه عن معرفة زودنا بها و كلما طلبنا كمية من وقته الثمين وفره لنا بالرغم من مسؤولياته المتعددة .

وإلى جميع أساتذتي ممن لم يتوانوا في مد يد العون لي طيلة سنوات دراستي

أهدي إليكم جميعا ثواب هذا الجهد والبحث فقد كنتم على الدوام ملهمي فعلى خطاكم أسير وبعلمكم أقتدي وبكم ينعقد العزم والقوة للخوض في ميادين العلم والحياة بعد التوكل على الله سبحانه وتعالى فجزاكم الله كل خير وأثابكم خير الجزاء .

حياة الهام

ملخص

في إطار هذه المذكرة، تم اختيار موضوع مراقبة ورصد الشبكة باستخدام أداة مجانية. تم اعتماد منصة ناجيوس كحل لتلك الغاية، نظرًا لقوتها ومرونتها وقدراتها الواسعة. يهدف هذا المشروع إلى توفير واجهة سهلة الاستخدام لتكوين ناجيوس وتخصيصها حسب احتياجات المستخدم. يتضمن ذلك إضافة وتعديل وتحديث معلومات الخوادم والخدمات وتعيين التنبيهات والتقارير وغيرها من الإعدادات الضرورية. يتوقع أن يسهم هذا المشروع في تحسين أداء مراقبة الشبكة وتعزيز الاستجابة والاستقرار في بيئة الشبكة .

Abstract

In the context of this dissertation, the topic of network monitoring and monitoring using a free tool has been chosen. Nagios platform has been adopted as a solution for this purpose, given its strength, flexibility, and extensive capabilities. The aim of this project is to provide a user-friendly interface for configuring and customizing Nagios according to user requirements. This includes adding, modifying, and updating server and service information, setting up alerts, reports, and other necessary settings. It is expected that this project will contribute to improving network monitoring performance and enhancing responsiveness and stability in the network environment

Résumé

Dans le cadre de ce mémoire, le sujet choisi concerne la surveillance et le suivi du réseau à l'aide d'un outil gratuit. La plateforme Nagios a été sélectionnée en raison de sa puissance, de sa flexibilité et de ses capacités étendues. L'objectif de ce projet est de fournir une interface conviviale pour configurer et personnaliser Nagios selon les besoins de l'utilisateur. Cela comprend l'ajout, la modification et la mise à jour des informations sur les serveurs, les services, la définition des alertes, les rapports et autres paramètres essentiels. Ce projet devrait améliorer les performances de surveillance du réseau, renforcer la réactivité et la stabilité de l'environnement réseau.

الكلمات المفتاحية :

المراقبة والرصد ، إدارة الشبكات، الشبكات ،ناجيوس، الأنظمة الافتراضية.

الفهرس

مقدمة عامة

الفصل الأول مراقبة الشبكات وأساسياتها

مقدمة 1

1- تعريف المراقبة ورصد الشبكات 2

2- أهمية المراقبة والرصد في الشبكات 2

3- الفرق بين مراقبة الشبكات والرصد 3

4- أنواع أدوات المراقبة الشبكات 3

4- 1 أدوات مراقبة الأداء 3

4- 2 أدوات رصد الشبكة 4

4- 3 أدوات إدارة الأخطاء 4

4- 4 أدوات إدارة التكوين 5

4- 5 أدوات الأمان 5

5- أنواع أدوات رصد الشبكة 6

5- 1 أدوات مراقبة البنية التحتية للشبكة 6

5- 2 أدوات مراقبة حركة البيانات 6

5- 3 أدوات مراقبة الأمان 7

5- 4 أدوات مراقبة الأداء 7

5- 5 أدوات مراقبة الجودة 8

5- مميزاتها 8

6- 1 مراقبة شاملة 8

6- 2 تنبيهات فورية 9

6- 3 سهولة الاستخدام 9

6- 4 تخطيط الشبكة 10

6- 5 تحليل الأداء 10

6- تحليل البيانات المستخرجة من أدوات المراقبة والرصد 11

7- استعمالات المراقبة الشبكة 11

8- 1 مراقبة الأداء 11

8- 2 الكشف عن الهجمات الإلكترونية 12

8- 3 تحسين أمان الشبكة 13

8- 4 التخطيط والتحليل 13

8- 5 إدارة النطاق الترددي 14

8- 6 الصيانة الوقائية 15
9- أهمية استخدام البرامج الحرة في عملية المراقبة والرصد 15
10- عملية تحليل الأداء والتحسين في مراقبة الشبكات والرصد 16
خاتمة 17

الفصل الثاني تحليل ومراجعة الأدوات المستخدمة في مراقبة الشبكة
مقدمة 18
1- عرض أدوات المراقبة والرصد الحرة 18
2- تعريف Nagios 19
3- خصائص برنامج ناجيوس (Nagios) 19
4- الوظائف 20
5- تصميم ناجيوس 21
6- ملحقات (Plugins) 22
7- الرصد السلبي والنشط 24
7- 1 المكونات النشطة NRPE 24
7- 2 المكونات السلبية NSCA 25
8- ملفات التكوين 25
خاتمة 26

الفصل الثالث تطبيق أداء شبكة الناجيوس باستخدام أدوات المراقبة والإشعارات
مقدمة 28
1- La virtualisation 28
1- 1 تعريفه 28
1- 2 ما هو الخادم الافتراضي؟ 29
1- 3 برنامجVirtual box 29
2- شرح كيفية تثبيت Ubuntuعلي virtuel box 30
3- شرح كيفية تثبيت Windowsعلي Virtuel Box 39
4- شرح كيفية تثبيت وإعداد برنامج الناجيوس على نظامUbuntu 45
4- 1 تعديل المنافذ 51
4- 2 أداة تحليل البيانات Nagios graph 52
5- كيفية استخدام أدوات المراقبة المختلفة المتاحة في الناجيوس 58
5- 1 NRPE 58
5- 1.1 تثبيته داخل ناجيوس 58

5- 1. 2 تثبيته داخل مستخدم 62
5- 2 NS Client++ 65
5- 1.2 تثبيته داخل المستخدم WINDOWS 65
5- 3 SNMP 68
5- 1.3 تعديل SNMP داخل Windows 68
5- 3. 2 إضافة windows إلى ناجيوس 71
6- كيفية إعداد الإشعارات لتلقي تنبيهات عند وجود مشكلات في الشبكة 74
6- 1 تعريف تطبيق تليجرام 74
6- 2إعداد تنبيهات لإرسال رسائل إلى تطبيق تيليجرام 74

خاتمة 83

خاتمة عامة

المراجع

قائمة الأشكال

الشكل رقم 1	يوضح عملية تجميع المعلومات والإشراف الشامل التي يقدمها ناجيوس لشبكة الحوسبة المركزية.	21
الشكل رقم 2	تصميم ناجيوس (Nagios)	22
الشكل رقم 3	مبدأ عمل الإضافات (plugins)	24
الشكل رقم 4	إنشاء جهاز افتراضي " Ubuntu"	30
الشكل رقم 5	تحديد حجم الذاكرة	30
الشكل رقم 6	إنشاء قرص صلب افتراضي	31
الشكل رقم 7	اختيار نوع القرص	31
الشكل رقم 8	اختيار زيادة حجم القرص الثابت	32
الشكل رقم 9	اختيار حجم القرص الثابت	32
الشكل رقم 10	مصدر التنزيل	33
الشكل رقم 11	بداية التثبيت	34
الشكل رقم 12	تثبيت Ubuntu	34
الشكل رقم 13	اختيار اللغة	35
الشكل رقم 14	اختيارات التثبيت	35
الشكل رقم 15	نهاية التثبيت	36
الشكل رقم 16	التسمية وإضافة كلمة السر	36
الشكل رقم 17	التثبيت	37
الشكل رقم 18	إعادة تشغيل الجهاز	37
الشكل رقم 19	الدخول	38
الشكل رقم 20	إدخال كلمة السر	38
الشكل رقم 21	إنشاء جهاز افتراضي windows	39
الشكل رقم 22	إنشاء قرص صلب افتراضي	40
الشكل رقم 23	اختيار نوع القرص	40
الشكل رقم 24	اختيار زيادة حجم القرص الثابت	40

الشكل رقم 25 اختيار حجم القرص الثابت	41
الشكل رقم 26 اختيار ISO WINDOWS 7	41
الشكل رقم 27 اختيار اللغة	42
الشكل رقم 28 بداية التثبيت	42
الشكل رقم 29 اختيار نوع النظام	43
الشكل رقم 30 نهاية التثبيت	43
الشكل رقم 31 اسم المستخدم	44
الشكل رقم 32 تعديل ال adresse ip	44
الشكل رقم 33 واجهة إدخال اسم المستخدم وكلمة السر	50
الشكل رقم 34 واجهة ناجيوس بعد استكمال التثبيت	50
الشكل رقم 35 واجهة ناجيوس الخارجية بعد إضافة graph	57
الشكل رقم 36 عرض ال graph	58
الشكل رقم 37 إضافة nrpe للإعدادات	60
الشكل رقم 38 التأكد من تشغيل Nagios	62
الشكل رقم 39 واجهة ناجيوس الخاصة بالمستخدم الأول " client "	64
الشكل رقم 40 تأكيد قبول الشروط	65
الشكل رقم 41 اختيار النوع	65
الشكل رقم 42 تثبيت إعدادات NS Client++	66
الشكل رقم 43 كتابة IP أو HOSTNAME خادم ناجيوس	66
الشكل رقم 44 ننتقل إلى ملف NS Client++	67
الشكل رقم 45 التحقق من وجود بعض التعليمات الخاصة بـ NS Client++	67
الشكل رقم 46 ننتقل إلى قائمة services	67
الشكل رقم 47 إعادة تشغيل NS Client++	68
الشكل رقم 48 تنشيط SNMP	69
الشكل رقم 49 البحث عن service snmp	69
الشكل رقم 50 إعداد الربط	70
الشكل رقم 51 ضبط حزم snmp	70

الشكل رقم 52 إعادة تشغيل SNMP 71

الشكل رقم 53 واجهة ناجيوس لمراقبة Windows 73
الشكل رقم 54 واجهة BotFather 75
الشكل رقم 55 بداية الاستعمال 75
الشكل رقم 56 إنشاء bot جديد و تحديد اسم له 76
الشكل رقم 57 رمز ال botToken الخاص بنا 76
الشكل رقم 58 إعدادات أضافية حتى يتمكن البوت من الانضمام تلقائيا للمجموعات الجديدة 77
الشكل رقم 59 اختيار Enable 77
الشكل رقم 60 التحقق 77
الشكل رقم 61 الدخول الي البوت خاص بنا و تشغيله 78
الشكل رقم 62 تيليجرام ID 78
الشكل رقم 63 البحث عن TelegramRaw bot وتشغيله 82
الشكل رقم 64 بدء استلام الإشعارات في البوت 83

قائمة الجداول

جدول رقم 1 معاني رموز العودة 23

الاختصارات

SNMP : Simple Network Management Protocol

IP SLA : IP Service Level Agreement

PRTG : Paessler Router Traffic Grapher

Nmap : Network Mapper

GFI : Groupe Français d'Informatique

TCP/IP : Transmission Control Protocol/Internet Protocol

SSH : Secure Shell

SMTP : Simple Mail Transfer Protocol

FTP : File Transfer Protocol

CPU : Central Processing Unit

POP3 : Post Office Protocol 3

HTTP : HyperText Transfer Protocol

NNTP : Network News Transfer Protocol

ICMP : Internet Control Message Protocol

LDAP: Lightweight Directory Access Protocol

SSL : Secure Sockets Layer

Bash : Bourne-Again shell
PHP : Hypertext Preprocessor

GUI : Graphical user interface

CGI : Common Gateway Interface

MySQL : My Structured Query Language

NRPE : Nagios Remote Plugin Executor

NSCA: National Strength and Conditioning Association

Mac : Media Access Contro

BSD : Banque de séquences didactiques

ISO : international Organization for Standardization

RAM : random access memory

VDI : Virtual desktop infrastructure

RRDtool : round-robin database tool

IP : Internet Protocol

BOT : robot

مقدمة عامة

مقدمة عامة

حاليًا، جميع الشركات مجهزة بشبكات محلية على الأقل، وشبكات بعيدة المدى للشركات الأكبر. تحتوي أجهزة حواسيبهم على عشرات أو حتى مئات المعدات، بما في ذلك خوادم قواعد البيانات وخوادم المعالجة. ونظرًا لأن هذه الأنظمة الحاسوبية تعتبر جوهرية لنشاطات الشركات، فإن التحكم فيها يصبح أمرًا حاسمًا. يجب أن تعمل هذه الأنظمة بكامل طاقتها وبشكل مستمر لضمان الموثوقية والكفاءة المطلوبتين، وخاصة في العمل على تقليل مشاكل الفشل والأعطال والانقطاعات والمشاكل التقنية المختلفة التي يمكن أن تتسبب في خسائر كبيرة.

وبالتالي، يلجأ مديرو شبكات الحاسوب إلى برامج المراقبة والرصد للشبكات للتحقق من حالة الشبكة في الوقت الحقيقي لمجمل الحواسيب المتواجدة تحت مسؤوليتهم، ويتم إعلامهم تلقائيًا (عن طريق البريد الإلكتروني أو الرسائل النصية) في حالة وجود أي مشكلات. وبفضل هذا النظام يتم تقليل الوقت اللازم للتدخلات بشكل كبير، ويمكن التعامل مع الأخطاء على الفور حتى قبل أن يلاحظها أحد المستخدمين.

وتعد المراقبة الشبكية ضرورية ولا غنى عنها. فهي تسمح من بين أمور أخرى بالحصول على رؤية عامة للوظيفة والمشاكل التي يمكن أن تنشأ على الشبكة، بالإضافة إلى الحصول على مؤشرات عن أداء بنيتها التحتية.

وفي هذا الإطار تعتمد هذه المذكرة على :

- ✓ مراقبة الشبكات وأساسياتها
- ✓ تحليل ومراجعة الأدوات المستخدمة في مراقبة الشبكة
- ✓ تطبيق أداء شبكة ناجيوس باستخدام أدوات المراقبة والإشعارات

الفصل الأول

مراقبة الشبكات وأساسياتها

الفصل الأول : مراقبة الشبكات وأساسياتها

مقدمة

يعد فصل مراقبة الشبكات وأساسياتها من أهم فصول علوم الحاسوب وتقنية المعلومات، حيث تعتبر المراقبة أحد الأسس الرئيسية في تطبيقات الشبكات وأنظمة المعلومات، إذ تساعد في الحفاظ على سلامة وأمان الشبكة وضمان أن أنظمة الشبكات تعمل بكفاءة وفعالية. وتتضمن أساسيات مراقبة الشبكيات عدة عناصر مثل مراقبة الأداء والجودة والأمان والتكوين وغيرها.

سيتناول الفصل الأساسيات الرئيسية لمراقبة الشبكيات، بدءًا من مقدمة حول مفهوم مراقبة الشبكات وأهميتها، ثم تعريف مصطلحات مراقبة الشبكات والتي تشمل الأداء والجودة والأمان والتكوين، ومن ثم سنتناول بالتفصيل كل عنصر من هذه المصطلحات وأدوات المراقبة المختلفة المتاحة في السوق لكل منها، بالإضافة إلى شرح كيفية استخدام هذه الأدوات وكيفية تحليل بيانات المراقبة واستخلاص المعلومات المفيدة منها.

بالإضافة إلى ذلك، سيتم التركيز على أهمية الصيانة الوقائية في مجال مراقبة الشبكات، حيث يتم شرح الإجراءات التي يجب اتخاذها لتفادي الأعطال والتحقق من سلامة النظام. كما سيتم الحديث عن أهمية تخطيط وتحليل الشبكة وكيفية استخدام بيانات المراقبة للتخطيط الفعال للنظام.

وبالإضافة إلى ذلك، سيتم التركيز على الأدوات المتاحة لإدارة النطاق الترددي والحفاظ على سرعة الشبكة، وكذلك أدوات كشف الهجمات الإلكترونية وعلى تحسين أمان الشبكة. سيتم أيضًا تغطية الصيانة الوقائية وأهميتها في الحفاظ على أداء الشبكة الجيد والحد من التوقفات المفاجئة.

تعتبر مراقبة الشبكات جزءًا أساسيًا من عمليات الإدارة التقنية للشركات والمؤسسات والمنظمات. وهي تساعد في الحفاظ على توافر الشبكة وأدائها الجيد، وتحسين الأمن السيبراني والحماية من الهجمات الإلكترونية. لذلك، فإن فهم أساسيات مراقبة الشبكات واستخدام الأدوات المتاحة لها يعد أمرًا ضروريًا لأي شخص يعمل في مجال تقنية المعلومات.

1-تعريف المراقبة ورصد الشبكات

تُعرف مراقبة الشبكة على أنها عملية مراقبة الأجهزة والخدمات الموجودة في شبكة الحاسوب، وتتضمن كذلك تحديد الأخطاء وإصلاحها وتحسين أداء الشبكة بشكل عام. وتعتبر المراقبة الشبكية أحد أهم جوانب إدارة الشبكات، حيث يساعد هذا النوع من المراقبة على الحد من الأعطال وتفاديها، وبالتالي تحسين الكفاءة والأداء العام للشبكة. وبفضل المراقبة الشبكية، يمكن للمسؤولين عن إدارة الشبكات الحصول على نظرة شاملة على حالة الشبكة ومستوى أدائها في الوقت الحقيقي، وتتيح لهم إجراء التغييرات والتعديلات اللازمة للحفاظ على سلامة واستقرار الشبكة.

أما رصد الشبكة فهو عملية مراقبة وتتبع حالة الشبكة ومكوناتها للتأكد من أنها تعمل بشكل صحيح وتحديد أي مشكلات تتطلب اتخاذ إجراءات فورية لتجنب توقف الخدمة. ويمكن تحقيق ذلك باستخدام أدوات رصد الشبكة المختلفة التي تتيح للمسؤولين على الشبكة مراقبة الأداء والموثوقية وتوفير الحلول في الوقت المناسب عند حدوث مشاكل. وتشمل هذه الأدوات مثلًا برامج مراقبة الشبكة وجهاز استشعار الشبكة وأجهزة قياس الأداء وتحليل البيانات وغيرها.[1]

2-أهمية المراقبة والرصد في الشبكات

تعتبر المراقبة والرصد في الشبكات من العوامل الحاسمة لتحسين أداء الشبكات وتشخيص المشكلات التي قد تواجهها. فالشبكات تعتبر العمود الفقري للكثير من الشركات والمؤسسات، وتوفر خدمات حيوية للمستخدمين والأجهزة المختلفة المتصلة بها . ومن هنا، يتعين على المسؤولين عن الشبكات والتقنيين والمهندسين المعنيين بالشبكات ضمان أن تعمل الشبكات بأفضل أداء ممكن وتحديد أي مشاكل قد تؤثر على أداء الشبكة وتقديم الحلول السريعة لتلك المشكلات.

حيث تتيح هذه الأدوات للمسؤولين عن الشبكات مراقبة العديد من المؤشرات المهمة مثل سرعة التحميل ،والكمية المنقولة من البيانات، الأداء العام للأجهزة المتصلة بالشبكة، والعديد من الأمور الأخرى. وباستخدام أدوات المراقبة والرصد الصحيحة، يمكن للمسؤولين عن الشبكات تحديد النقاط الضعيفة في الشبكة والعمل على تحسينها قبل أن تتسبب في مشاكل أكبر وتعيق أداء الشبكة.

ومن أهميتها أيضاً هي قدرتها على تشخيص المشكلات التي قد تواجه الشبكة، وتحديد أسبابها وحلها بأسرع وقت ممكن. فعندما تظهر مشكلة في الشبكة، فإن أدوات المراقبة والرصد تقوم بتحليل البيانات وتحديد أسباب المشكلة، وبالتالي يمكن للمسؤولين عن الشبكة إيجاد الحلول .

3- الفرق بين مراقبة الشبكات والرصد

يشير مصطلح "مراقبة الشبكات" إلى عملية مراقبة الأنظمة والأجهزة والخدمات الموجودة في الشبكة، وذلك لضمان أداء مستقر وفعالية عالية. ويشمل ذلك مراقبة البنية التحتية للشبكة، ومتابعة الأجهزة والتطبيقات للتأكد من سلامتها واستجابتها بشكل صحيح، وكذلك تحديد الأعطال وإصلاحها.

أما "الرصد" فهو يعني تحليل النظام بشكل مستمر لمعرفة ما إذا كان يعمل بشكل جيد أم لا، وتحديد أي تغييرات غير متوقعة في النظام أو المستخدمين، والتنبيه عند حدوث أي مشكلة أو خلل في النظام. ويتم ذلك عادة عن طريق تحليل البيانات المستمرة التي تجمع من الأجهزة والخدمات المختلفة في الشبكة، ومقارنتها بالسلوك الطبيعي للنظام.

وبشكل عام، يمكن القول أن "مراقبة الشبكات" تهدف إلى الحفاظ على أداء الشبكة عند أقصى مستوى من الكفاءة، بينما يهدف "الرصد" إلى التعرف على المشكلات وحلها قبل أن تؤثر على أداء النظام بشكل كبير.

4-أنواع أدوات مراقبة الشبكات

توجد العديد من أنواع أدوات المراقبة الشبكية ومنها:

4- 1 أدوات مراقبة الأداء

يشمل مجال مراقبة الأداء في الحوسبة جميع الأدوات والتقنيات التي تستخدم لرصد وتقييم أداء النظام والتطبيقات وتحديد مصادر الأداء المحتملة. تساعد أدوات مراقبة الأداء على تحسين أداء النظام وتجنب المشكلات والأعطال التي يمكن أن تؤثر على استجابة التطبيقات وجودة الخدمة. ويتم ذلك عن طريق جمع البيانات وتحليلها لتقديم معلومات مفصلة حول أداء النظام والتطبيقات وتحديد أين يمكن العثور على أي مشاكل في النظام. يمكن استخدام أدوات مراقبة الأداء للشبكات والخوادم ونظام التشغيل والتطبيقات. وتختلف أدوات مراقبة الأداء من حيث الوظائف والميزات التي تقدمها، وتشمل بعضها التنبيهات الفورية وتقارير التحليل والرسوم البيانية لعرض بيانات الأداء بطريقة سهلة الفهم[5]

4- 2 أدوات رصد الشبكة

تعد أدوات رصد الشبكةNetwork Monitoring Tools من الأدوات الهامة التي تستخدم للتحكم والإشراف على شبكات الحاسوب ومراقبة حركة البيانات وأداء الأجهزة المتصلة بها. فهي تعتبر أدوات مهمة جدا لأي شبكة، سواء كانت كبيرة أو صغيرة، لأنها تساعد في الحفاظ على استقرار الشبكة وتحسين أدائها وتجنب الأخطاء المحتملة والمشاكل التي يمكن أن تؤدي إلى توقف الخدمة.

تتضمن أدوات رصد الشبكة مجموعة من الأدوات المختلفة مثل أدوات مراقبة حركة البيانات وأدوات تحليل الأداء وأدوات مراقبة الأجهزة والخوادم والتطبيقات والخدمات. تقوم هذه الأدوات بجمع البيانات وتحليلها وعرضها بطريقة سهلة الاستخدام لمساعدة المسؤولين على تحليل البيانات واتخاذ الإجراءات المناسبة.

ومن أهم مميزات أدوات رصد الشبكة هي قدرتها على تحديد أي جهاز متصل بالشبكة والتحقق من حالة تشغيله، وتحليل حركة البيانات وتحديد المناطق التي توجد فيها مشكلات ومن ثم توفير إحصائيات تفصيلية حول أداء الشبكة والأجهزة المختلفة. ويمكن استخدام هذه البيانات لتحديد الأخطاء المحتملة والتصرف فيها بسرعة قبل أن تؤدي إلى مشاكل أكبر.

وفي النهاية، فإن أدوات رصد الشبكة هي أدوات أساسية لأي مسؤول شبكة، حيث تساعدهم في مراقبة وإدارة الشبكة بكفاءة وتحسين أدائها وضمان عمليات الاتصال المستمرة. [5]

4- 3 أدوات إدارة الأخطاء

أدوات إدارة الأخطاء هي أدوات تساعد على تحديد وإصلاح الأخطاء التي تظهر في الشبكة والأنظمة. بحيث عندما يحدث خطأ في الشبكة، فإن هذه الأدوات تتيح للمسؤولين عن النظام تحديد المكان الذي يحتاج إلى الإصلاح وتصحيح المشكلة بسرعة وكفاءة. تستخدم هذه الأدوات بشكل واسع في الشبكات الكبيرة والمعقدة، حيث يمكن أن يكون من الصعب تحديد مصدر الخطأ يدويًا.

وتشمل العديد من الخيارات مثل إصلاح الأخطاء تلقائيًا، وإنشاء تقارير الأخطاء وإرسال تنبيهات عند حدوث أخطاء محددة، وتوفير إحصائيات حول الأخطاء والأداء. كما أنها تتيح للمسؤولين عن النظام تحليل البيانات المتعلقة بالأخطاء والأداء لتحديد مصادر المشاكل والعمل على تحسين النظام بشكل عام.[2]

4-4 أدوات إدارة التكوين

أدوات إدارة التكوين (Configuration Management Tools) هي أدوات تستخدم لإدارة تكوين الأنظمة والتطبيقات المختلفة في بيئة الحوسبة السحابية والأنظمة الموزعة. تعمل هذه الأدوات على توفير إمكانية تكرار عمليات التثبيت والتكوين والإصدار، وتساعد على تقليل الأخطاء وزيادة الاستجابة والأمان في النظام.

تعد أدوات إدارة التكوين من الأدوات الحيوية في إدارة الأنظمة والتطبيقات، حيث توفر الكثير من المزايا مثل:

- توفير وسائل تحكم وإدارة شاملة لتكوين الأنظمة والتطبيقات .
- تقليل الوقت والجهد اللازم لتثبيت وتكوين الأنظمة والتطبيقات .
- تقليل عدد الأخطاء المحتملة والتي يمكن أن تؤثر على النظام .
- تقليل الاستجابة في تحديث وتغيير التكوين، حيث يمكن تطبيق التحديثات على عدة أجهزة في وقت واحد .
- زيادة الأمان في النظام، حيث يمكن التحكم بالتكوين بطريقة مركزية ومن خلال سياسات أمان محددة.

ويوجد العديد من أدوات إدارة التكوين المستخدمة في بيئة الحوسبة السحابية والأنظمة الموزعة، مثل Ansible و Puppet و Chef وSaltStack وغيرها. وتختلف هذه الأدوات في الطريقة التي تعمل بها والميزات التي توفرها، حيث يمكن اختيار الأداة المناسبة بناءً على الاحتياجات المحددة للنظام أو التطبيق. [5]

5-4 أدوات الأمان

أدوات الأمان هي عبارة عن مجموعة من البرامج والأدوات التي تستخدم لضمان أمان البيانات والمعلومات الموجودة داخل الشبكة. ويعد أمان الشبكات والمعلومات من أهم الأمور التي يجب الاهتمام بها في أي شركة أو مؤسسة تعتمد على الشبكات وتكنولوجيا المعلومات في عملياتها اليومية.

توفر أدوات الأمان وسائل متعددة لحماية الشبكات والأجهزة من التهديدات الأمنية المختلفة، مثل الفيروسات والبرمجيات الخبيثة والاختراقات السيبرانية والهجمات الإلكترونية الأخرى. وتتضمن هذه الأدوات على سبيل المثال لا الحصر جدران الحماية (Firewalls) وبرامج مكافحة الفيروسات وأدوات الكشف عن الاختراق (Intrusion Detection Systems) وغيرها.[5]

بالإضافة إلى ذلك، تعمل أدوات الأمان على حماية البيانات الحساسة من التسريب والسرقة، ويشمل ذلك أيضًا آليات التشفير والتوقيع الرقمي وأدوات إدارة الهوية والوصول (Identity and Access Management).

وتتفاوت أدوات الأمان فيما بينها من حيث الوظائف والميزات والتقنيات المستخدمة، ويتوجب على المسؤولين عن أمن الشبكات اختيار الأدوات الأكثر تناسبًا مع احتياجات الشركة وميزانية الأمن المخصصة لذلك.

يجب ملاحظة أن هذه الأدوات ليست شاملة لجميع أنواع أدوات المراقبة الشبكية المتاحة، حيث يمكن أن يتم تصنيفها حسب العديد من المعايير، بما في ذلك الغرض الرئيسي للاستخدام ونطاق الشبكة ونوعية البيانات المراد جمعها. [5]

5-أنواع أدوات رصد الشبكة

هناك عدة أنواع من أدوات رصد الشبكة، ومن بينها:

5- 1 أدوات مراقبة البنية التحتية للشبكة

أدوات مراقبة البنية التحتية للشبكة هي مجموعة من الأدوات التي تساعد في رصد ومراقبة أجهزة الشبكة والبنية التحتية المختلفة المرتبطة بها. تتضمن هذه الأدوات مراقبة الأجهزة المادية مثل السيرفرات والراوترات والسويتشات، بالإضافة إلى أدوات مراقبة البرامج والخدمات التي تعمل على الأجهزة المادية، مثل قواعد البيانات وخوادم الويب والبريد الإلكتروني وغيرها.

تعتمد أدوات مراقبة البنية التحتية للشبكة على عدد من التقنيات والبروتوكولات المختلفة، مثل SNMP (Simple Network Management Protocol) و NetFlow و IP SLA وغيرها، وتوفر هذه الأدوات إمكانية الوصول إلى بيانات الأجهزة والخدمات ومراقبتها وتحليلها وإعداد تقارير عن حالة الشبكة ومستوى الأداء. وتعتبر أدوات مراقبة البنية التحتية للشبكة أساسية لتحسين تجربة المستخدم وتوفير الأداء الأمثل للشبكة.[5]

5- 2 أدوات مراقبة حركة البيانات

أدوات مراقبة حركة البيانات هي الأدوات التي تتيح للمسؤولين عن الشبكات مراقبة حركة البيانات داخل الشبكة. تتيح هذه الأدوات رصد حجم البيانات المرسلة والمستقبلة، وكذلك معدل البيانات في الوقت الحقيقي وسرعة نقل البيانات. يتم استخدام هذه الأدوات عادة للكشف عن أي أنماط غير عادية في حركة

البيانات ولتحديد مواقع التكدس والاختناقات في الشبكة، مما يتيح للمسؤولين إصلاح المشاكل بشكل فعال وتحسين أداء الشبكة بشكل عام. أمثلة على أدوات مراقبة حركة البيانات :

PRTG Network Monitor و Net Flow Analyzer و SolarWinds Network Traffic Analyzer

5- 3 أدوات مراقبة الأمان

أدوات مراقبة الأمان هي مجموعة من البرامج التي تستخدم لتحليل سجلات الأحداث ومراقبة النظام والتنبيه عن أي تهديدات أمنية محتملة. وتعد هذه الأدوات أساسية لأي منظومة معلوماتية لأنها تساعد في تحسين الأمن وحماية البيانات والمعلومات من الاختراقات والهجمات الإلكترونية. تقوم هذه الأدوات بمراقبة الشبكات والأنظمة والتطبيقات، وتوفر تحليلات وتقارير مفصلة عن أي تهديدات أمنية تم اكتشافها، كما تساعد في اتخاذ إجراءات سريعة وفعالة لمعالجة تلك التهديدات.

تتضمن أدوات مراقبة الأمان العديد من الميزات مثل الكشف عن الاختراقات، والكشف عن الفيروسات وبرامج التجسس، والكشف عن الهجمات الإلكترونية، والكشف عن المخترقين ومصادر الهجمات، والكشف عن الثغرات الأمنية في الأنظمة والتطبيقات. وتعمل هذه الأدوات على مراقبة جميع الأحداث الأمنية والتحقق من سلامة الملفات والبرامج المستخدمة، وتزويد المستخدمين بتقارير مفصلة عن حالة الأمان الخاصة بالنظام والشبكة.

تتمثل أشهر أدوات مراقبة الأمان في :

Snortو Nessus وSecurity Onion وWiresharkوGFI LanGuard وNmapو SolarWinds Security Event Managerوغيرها.

5-4 أدوات مراقبة الأداء

أدوات مراقبة الأداء هي مجموعة من البرامج والأنظمة التي تستخدم لرصد أداء الشبكة والحواسيب والتطبيقات. تساعد هذه الأدوات على تحديد المشكلات المحتملة في الأداء وتحسين الأداء وزيادة كفاءة النظام بشكل عام. تتيح للمسؤولين عن الشبكة والحواسيب معرفة أين يمكن تحسين الأداء وتحسين استجابة التطبيقات، ومعالجة المشكلات قبل أن تتسبب في توقف النظام.

تشمل أدوات مراقبة الأداء مجموعة متنوعة من البرامج والأنظمة، بما في ذلك برامج مراقبة الشبكة، وبرامج تحليل الأداء، وبرامج مراقبة الخادم، وبرامج تحليل البيانات، والعديد من الأدوات

الأخرى. يتم استخدام هذه الأدوات لقياس عدد من المعايير الأساسية لأداء النظام، مثل سرعة الاتصال، وزمن الاستجابة، وحجم البيانات المنقولة، والقدرة على تحمل الأعباء الثقيلة.

تتميز أدوات مراقبة الأداء بقدرتها على إنشاء تقارير مفصلة عن أداء النظام والتطبيقات، وتوفير البيانات المتعلقة بالاستخدام والأداء، وتقديم إحصائيات مفصلة حول أداء النظام والخوادم. كما أنها تتيح للمستخدمين الحصول على تحليل شامل لأداء النظام والتطبيقات، والكشف عن المشاكل المحتملة في الوقت الحقيقي.

يمكن استخدام أدوات مراقبة الأداء في العديد من المجالات، مثل الشركات والمؤسسات والمواقع الإلكترونية والتطبيقات.

5- 5 أدوات مراقبة الجودة

أدوات مراقبة الجودة هي عبارة عن مجموعة من الأدوات والتقنيات التي تساعد على تحديد مستوى الجودة في عملية الإنتاج أو الخدمات المقدمة. تستخدم هذه الأدوات في العديد من المجالات مثل صناعة السيارات والطيران والتصنيع الغذائي والتكنولوجيا والرعاية الصحية والخدمات المالية وغيرها.

تعتبر أدوات مراقبة الجودة جزءًا هامًا من عملية الإدارة الفعالة، فهي تمكّن الشركات والمؤسسات من تحقيق أهدافها في تحسين الجودة وتوفير الموارد وتحسين الكفاءة. تتضمن هذه الأدوات مجموعة واسعة من الأدوات والتقنيات مثل مخططات الرسم البياني والمحاكاة وتحليل الأسباب الجذرية والمسح الإحصائي للعمليات.

ومن بين الأدوات الشهيرة في مراقبة الجودة، نجد أدوات قياس الجودة والتحكم فيها وتحليلها وتحليل البيانات. وتتوفر هذه الأدوات في العديد من البرامج والتطبيقات المختلفة التي تستخدم في الشركات والمؤسسات لتحسين جودة منتجاتهم أو خدماتهم.

6-مميزاتها

هناك العديد من المميزات التي تتوفر في أدوات المراقبة الشبكية، ومنها:

6- 1 مراقبة شاملة

تُعد المراقبة الشاملة (End-to-End Monitoring) من أهم الأساليب التي يتم استخدامها في

مراقبة الأنظمة الحاسوبية والشبكات. تُستخدم هذه الطريقة للتأكد من جودة أداء النظام وتوافره، وتتضمن مراقبة كافة العناصر التي يتألف منها النظام والتأكد من أنها تعمل بشكل صحيح وبكفاءة عالية.

تتضمن المراقبة الشاملة عادةً عدة أدوات وتقنيات لجمع وتحليل البيانات، مثل أدوات الرصد والتحليل، والتي يمكن استخدامها لمراقبة عملية نقل البيانات بين الخوادم والعملاء، وقياس الأداء، وتحديد المشاكل والأخطاء التي تؤثر على جودة الخدمة المقدمة.

يمكن استخدام المراقبة الشاملة في مجالات مختلفة، مثل الشركات والمؤسسات والمواقع الإلكترونية وتطبيقات الهواتف الذكية وغيرها، ومن أهم مزايا استخدام هذه الأدوات هو تحسين أداء النظام وزيادة توافره، وتحسين جودة الخدمة المقدمة للمستخدمين، وتقليل فترات التوقف غير المخططة وتحديد مصادر المشاكل بشكل سريع وفعال.[2]

6- 2 تنبيهات فورية

تعد التنبيهات الفورية (Immediate Alerts) أحد الأدوات الهامة في مراقبة الشبكات والأنظمة، وهي تستخدم لتوفير رصد مستمر للأحداث الهامة والتنبيه بشكل فوري في حالة حدوث أي عطل أو خلل أو انحراف عن الحالة الطبيعية للنظام. وتتميز تلك الأداة بسرعة الاستجابة والتحذير المبكر للمسؤولين عن الشبكات، مما يسمح لهم باتخاذ إجراءات الصيانة والإصلاح اللازمة في الوقت المناسب.

تقوم تلك الأداة بتحليل الأحداث المسجلة في النظام باستمرار، وتستخدم العديد من التقنيات لكشف أي خلل أو مشكلة قد تواجه النظام. ويمكن ضبط هذه التنبيهات لتناسب متطلبات المستخدم، حيث يمكن تعيين المعايير اللازمة لإطلاق التنبيهات في حالة تجاوز أي عتبة محددة.

تستخدم التنبيهات الفورية في العديد من المجالات، بما في ذلك المجالات الصناعية والتجارية والتقنية، حيث يمكن استخدامها في مراقبة شبكات الحاسوب والخوادم والتطبيقات والأنظمة، وكذلك لمراقبة أجهزة الاستشعار وأجهزة القياس والمراقبة في الصناعات المختلفة. وتساعد تلك الأداة على الحد من الأعطال والتوقفات غير المتوقعة، وبالتالي تحسين أداء النظام وزيادة كفاءته.

6- 3 سهولة الاستخدام

سهولة الاستخدام تعتبر واحدة من أهم الميزات، حيث يتطلب استخدام هذه الأدوات من قبل فريق تقني مختص له القدرة على التحكم فيها بشكل سهل ومرن. وبالتالي، فإن وجود واجهة سهلة الاستخدام يسهل عملية تحليل البيانات وجعلها مفهومة ومتاحة لجميع أعضاء الفريق المسؤول عن إدارة الشبكة.

كما يجب أيضًا أن تتميز هذه الأدوات بتنبيهات فورية ودقيقة، حيث تسمح بإعلام الفريق المسؤول عن إدارة الشبكة بأية مشكلة أو خلل قد يحدث في الوقت الفعلي، مما يسهل عملية التدخل والتصحيح قبل أن يتسبب الخلل في أي أضرار.

وبالإضافة إلى ذلك، يتطلب استخدام هذه الأدوات للمراقبة والرصد في الشبكات الكبيرة، وهذا يعني وجود العديد من الأجهزة والمكونات المختلفة التي يجب مراقبتها ورصدها. ولهذا السبب، يجب أن تتوفر هذه الأدوات على ميزة المراقبة الشاملة، حيث يمكنها مراقبة جميع أجزاء الشبكة وتحليلها بكفاءة ودقة.

6- 4 تخطيط الشبكة

تخطيط الشبكة هو عملية تصميم وتنظيم هيكلية الشبكة، بما في ذلك تحديد المكونات الأساسية للشبكة مثل الأجهزة والبرامج والبروتوكولات والخدمات المستخدمة. يتطلب تخطيط الشبكة فهماً عميقاً لمتطلبات الشبكة وأهدافها، بالإضافة إلى التحليل الدقيق للاحتياجات الحالية والمستقبلية للمستخدمين والتطبيقات المستخدمة.

تخطيط الشبكة يشمل العديد من الأنشطة التي تهدف إلى تصميم وتوزيع المكونات الشبكية بطريقة مثلى، مثل تحديد متطلبات الشبكة، وتحديد المكونات الأساسية للشبكة، وتحديد طوبولوجيا الشبكة، وتحديد بروتوكولات الاتصال، وتصميم نموذج الأمان، وتوزيع العتاد والبرامج والموارد، وتوثيق الشبكة.

أدوات تخطيط الشبكة توفر مجموعة من الخدمات والميزات التي تساعد في تخطيط وتصميم الشبكة بطريقة مثلى وفعالة. تشمل هذه الأدوات تقنيات تحليل البيانات وتصميم الشبكة، وتكنولوجيا النمذجة والمحاكاة، وأدوات تصميم وتحرير طوبولوجيا الشبكة، وأدوات تحديد المشاكل وإصلاحها، وأدوات التحليل الأمني وتحديد الثغرات وإغلاقها.

تتيح أدوات تخطيط الشبكة للمسؤولين عن الشبكة القدرة على تحديد المكونات المناسبة للشبكة وتحديد متطلبات الأداء والسعة والأمان، وضمان تصميم شبكة فعالة ومستقرة وآمنة. كما تساعد هذه الأدوات في تقليل التكاليف .

6- 5 تحليل الأداء

تحليل الأداء هو عملية تقييم وقياس أداء النظام أو التطبيق في بيئة محددة. ويهدف تحليل الأداء إلى تحديد الأخطاء والتحسينات اللازمة لتحسين أداء النظام وتوفير أفضل تجربة للمستخدمين.

وتعتبر أدوات مراقبة الأداء من أهم الأدوات المستخدمة في تحليل الأداء، حيث تساعد في قياس وتحليل الأداء الفعلي للشبكة أو التطبيق وتحديد المشاكل والعثور على الحلول اللازمة لها. وتوفر هذه الأدوات بيانات دقيقة وشاملة حول استخدام الموارد وحركة البيانات ومدى تأثير ذلك على الأداء.

وتتضمن أدوات تحليل الأداء عدة ميزات، مثل توفير الإحصائيات المفصلة والرسوم البيانية والتقارير المتعلقة بأداء النظام أو التطبيق، وتوفير تحليلات في الوقت الحقيقي والتنبيهات المباشرة في حالة حدوث مشكلات في الأداء، وتوفير تقارير مفصلة حول الأداء على فترات زمنية مختلفة.

ويمكن استخدام أدوات تحليل الأداء في العديد من المجالات، مثل الشركات والمؤسسات والمواقع الإلكترونية والتطبيقات. ومن أهم استخدامات هذه الأدوات تحسين أداء النظام أو التطبيق وتقليل الأخطاء والتأكد من توفير تجربة أفضل للمستخدمين وتحسين كفاءة العمليات وتحقيق الإنتاجية .

7-تحليل البيانات المستخرجة من أدوات المراقبة والرصد

تحليل البيانات المستخرجة من أدوات المراقبة والرصد يعد جزءًا مهمًا من عملية إدارة الشبكات والحفاظ على استدامتها وتشغيلها بشكل فعال. تعتمد هذه العملية على جمع وتحليل البيانات المتعلقة بأداء الشبكة، والمرور على تلك البيانات لتحديد الأنماط السلبية والتحسينات المطلوبة.

وتشمل البيانات التي يتم جمعها وتحليلها في هذه العملية على سبيل المثال لا الحصر: معدلات النقل وسرعة البيانات وعرض النطاق الترددي، وعدد الحوادث المسجلة ومعدلات الاستجابة وحالة الخادم، ومعدلات الطلبات والاستجابات وتوزيع الأحمال.

وبعد جمع هذه البيانات، يتم تحليلها وتقديمها بطريقة منظمة ومفيدة باستخدام أدوات تحليل البيانات، مثل الرسوم البيانية والتقارير والمخططات. ومن خلال تحليل هذه البيانات، يتم تحديد العقبات والمشكلات التي تؤثر على أداء الشبكة ويتم اتخاذ الإجراءات اللازمة لإصلاحها وتحسين الأداء بشكل عام.

8-استعمالات المراقبة الشبكية

تتضمن استخدامات المراقبة الشبكية عدة مجالات وأهداف ومن أهم هذه الاستخدامات:

8- 1 مراقبة الأداء

مراقبة الأداء Performance Monitoring هي عملية رصد وتحليل وقياس أداء النظام الحاسوبي أو الشبكة ومكوناتها بشكل مستمر ومنتظم، وذلك بهدف تحديد أي عوامل قد تؤثر على أداء النظام وتقليل حدوث الأعطال والمشاكل التي قد تؤدي إلى انقطاع الخدمات أو التأخير في تقديمها.

تتضمن مراقبة الأداء مجموعة من الأدوات والتقنيات التي تساعد على رصد وتحليل أداء النظام، وتشمل هذه الأدوات البرمجيات المختلفة والأجهزة المتخصصة في المراقبة والقياس.

تعد مراقبة الأداء أمرًا حيويًا في عالم الشبكات والحوسبة، حيث يتم تطبيقها بشكل كبير في الشركات والمؤسسات لتحسين أداء النظام وضمان استمرارية الخدمات، كما يتم استخدامها في المواقع الإلكترونية والتطبيقات لضمان توفر الخدمات للمستخدمين بأفضل أداء ممكن.

يمكن استخدام أدوات مراقبة الأداء لقياس الأداء في مختلف المجالات، بما في ذلك أداء الأنظمة الحاسوبية، وأداء الشبكات، وأداء قواعد البيانات، وأداء الخوادم، وغيرها من المجالات التي تتطلب مراقبة الأداء والتحكم فيه.

تحتوي أدوات مراقبة الأداء على العديد من الميزات والوظائف، وتمكن المستخدمين من تحديد المشكلات والأخطاء التي تؤثر على أداء النظام وتتبعها بشكل فوري، كما تساعد على تنبيه المستخدمين في حالة وجود مشكلة أو انخفاض في الأداء، مما يساعد على اتخاذ الإجراءات اللازمة لتحسين الأداء .

8- 2 الكشف عن الهجمات الإلكترونية

في الوقت الحالي، أصبحت الهجمات الإلكترونية شيئًا يواجهه العديد من الأفراد والمؤسسات بشكل يومي، وقد تسببت في خسائر مالية وتسريب بيانات حساسة وتعطيل الخدمات. ولحماية المؤسسات والأفراد من هذه الهجمات الإلكترونية، تعتبر أدوات الكشف عن الهجمات الإلكترونية من أهم الأدوات التي يمكن استخدامها.

تعمل أدوات الكشف عن الهجمات الإلكترونية على تحليل حركة المرور على الشبكة ورصدها بحثًا عن أي نشاط غير معتاد يمكن أن يشير إلى هجوم إلكتروني. كما تستخدم هذه الأدوات تقنيات الذكاء الاصطناعي وتعلم الآلة تحليل البيانات وتحديد أي نوع من الهجمات قد يتم استخدامها.

بالإضافة إلى ذلك، فإن أدوات الكشف عن الهجمات الإلكترونية تساعد على رصد الهجمات الجديدة وتحليلها وتطوير آليات لمواجهتها في المستقبل. وبفضل هذه الأدوات، يمكن للمؤسسات الاستجابة بسرعة لأي هجوم إلكتروني واتخاذ التدابير اللازمة لحماية بياناتهم وأصولهم.

يمكن استخدام أدوات الكشف عن الهجمات الإلكترونية في مجالات عديدة، مثل الشركات والمؤسسات والحكومات والمؤسسات الصحية والمالية. وتتوفر هذه الأدوات عادةً على شكل برامج تثبت على أجهزة الكمبيوتر أو الخوادم أو يمكن استخدامها كخدمة سحابية.

يجب الانتباه إلى أن أدوات الكشف عن الهجمات الإلكترونية ليست كافية لحماية المؤسسات والأفراد .

8- 3 تحسين أمان الشبكة:

تحسين أمان الشبكة هو أحد أهم الأولويات في عالم تقنية المعلومات والاتصالات، حيث يعتبر الأمن جزءًا أساسيًا من استدامة العمليات التجارية والحفاظ على سلامة البيانات والمعلومات الحساسة. ولتحسين أمان الشبكة، يتم استخدام مجموعة متنوعة من الأدوات والتقنيات التي تهدف إلى توفير الحماية والأمان للنظام والمعلومات المتبادلة عبر الشبكة.

تعتبر أدوات مراقبة الأمان من أهم هذه الأدوات، حيث تتيح للمسؤولين عن الشبكة مراقبة الأنشطة غير المصرح بها والكشف عن أي تهديدات أمنية محتملة. كما تساعد في اكتشاف وتحليل السلوكيات الغريبة على الشبكة، مثل محاولات الاختراق والبرامج الضارة وغيرها من الهجمات الإلكترونية.

ومن أهم الأدوات المستخدمة لتحسين أمان الشبكة نذكر:

- **أدوات كشف الاختراق(Intrusion Détection System)** التي تستخدم لمراقبة حركة البيانات في الشبكة والكشف عن أي أنشطة غير مصرح بها أو مشبوهة، ويمكنها إعلام المسؤولين بالأنشطة غير المصرح بها بشكل فوري.
- **أدوات إدارة الهوية والوصول(Identity and Access Management)**التي تستخدم لإدارة حقوق الوصول للمستخدمين في الشبكة، وتحديد ما إذا كان بإمكانهم الوصول إلى المعلومات الحساسة أم لا.
- **أدوات التشفير** (**Encryption**)التي تستخدم لتشفير البيانات وجعلها غير قابلة للاختراق، مما يساعد على حماية البيانات من الوصول غير المصرح به.

8- 4 التخطيط والتحليل:

أدوات التخطيط والتحليل هي أدوات متخصصة تساعد في تخطيط وتحليل مختلف العمليات والمشاريع. تستخدم هذه الأدوات عادة في مجالات الأعمال والهندسة والعلوم والتكنولوجيا والعديد من المجالات الأخرى التي تتطلب التخطيط والتحليل.

تشمل أدوات التخطيط والتحليل مجموعة متنوعة من الأدوات التي تتيح للمستخدمين تقييم العديد من العوامل والمعطيات والتنبؤ بالنتائج المستقبلية. تشمل هذه الأدوات تحليل البيانات، والنمذجة، والتنبؤ، والإحصاء، والتحليل الاقتصادي، والتخطيط الاستراتيجي، وغيرها.

تعتمد فاعلية أدوات التخطيط والتحليل على جودة المعلومات التي تدخل في هذه الأدوات. وبالتالي فإن جودة النتائج المتوقعة تعتمد على الدقة والشمولية والصحة و الصحة النسبية للبيانات التي تستخدم في هذه الأدوات.

تستخدم أدوات التخطيط والتحليل على نطاق واسع في العديد من المجالات، بما في ذلك التخطيط الاستراتيجي، وإدارة المشاريع، والتحليل الاقتصادي، وإدارة العمليات، وتحليل البيانات، وغيرها. ويتم استخدام هذه الأدوات لتوفير القرارات الدقيقة والتوقعات الدقيقة التي يمكن استخدامها في تحسين الأداء وزيادة الإنتاجية والتحكم في التكاليف وتحسين جودة المنتجات والخدمات وتحسين تجربة العملاء.

8-5 إدارة النطاق الترددي:

إدارة النطاق الترددي (Bandwidth Management) هي عملية تخصيص وإدارة النطاق الترددي في شبكة الحاسوب. يتم استخدام النطاق الترددي لقياس كمية البيانات التي يتم نقلها عبر شبكة الحاسوب خلال وحدة زمنية محددة. وتعد إدارة النطاق الترددي أمرًا حيويًا لتحسين أداء شبكات الحاسوب وضمان توافر الخدمات المتوقعة للمستخدمين.

يتم تحقيق إدارة النطاق الترددي عن طريق وضع حدود على كمية النطاق الترددي المخصصة لكل جهاز أو تطبيق في الشبكة. ويتم ذلك باستخدام أدوات الإدارة التي توفرها العديد من أنظمة الشبكات، والتي تسمح للمسؤولين بتحديد أولويات الاستخدام وتحديد الحد الأقصى لسرعة الاتصال بين الأجهزة المختلفة في الشبكة.

تتضمن أدوات إدارة النطاق الترددي العديد من الوظائف الأساسية، مثل قياس استخدام النطاق الترددي للتطبيقات المختلفة وتحليل البيانات المتعلقة بحركة المرور وتحديد مستويات الأولوية وإعداد القيود والقواعد لتحسين توزيع النطاق الترددي.

بشكل عام، يساعد تطبيق إدارة النطاق الترددي على تحقيق العديد من المزايا، بما في ذلك تحسين أداء الشبكة وتحسين توافر الخدمات المتوقعة للمستخدمين وتحسين استخدام النطاق الترددي وتوزيعه بين الأجهزة والتطبيقات المختلفة والحد من الازدحام في الشبكة والتحكم في استخدام النطاق الترددي من قبل المستخدمين والتطبيقات.

8-6 الصيانة الوقائية:

تعد الصيانة الوقائية (Preventive Maintenance) من أهم الخطوات التي يجب اتخاذها للحفاظ على الأنظمة والمعدات في حالة جيدة، وتجنب التعطيلات غير المتوقعة التي قد تتسبب في توقف العمل وخسارة الوقت والمال. تهدف الصيانة الوقائية إلى تحديد الأعطال المحتملة وإصلاحها قبل حدوثها، وتتضمن فحص الأنظمة والمعدات بشكل دوري وتنظيفها وتزويدها بالزيوت والشحوم والقطع الاستهلاكية اللازمة.

تشمل الصيانة الوقائية العديد من الأنشطة والممارسات، مثل:

- تنظيف الأنظمة والمعدات بشكل دوري لإزالة الأتربة والشوائب التي قد تؤدي إلى تلفها.
- فحص الأنظمة والمعدات بشكل دوري للتأكد من سلامتها وصلاحيتها للاستخدام، ويمكن استخدام أدوات الاختبار المختلفة لهذا الغرض.
- تزويد الأنظمة والمعدات بالزيوت والشحوم والقطع الاستهلاكية اللازمة لتحسين أدائها وتقليل الاهتراء .
- تنفيذ الصيانة الدورية والمنتظمة للأجزاء الحيوية في الأنظمة والمعدات، مثل تغيير الفلاتر والأنابيب والأسلاك الكهربائية.
- تحديث البرامج والتطبيقات بشكل دوري لتحسين أدائها ومواكبة التطور التكنولوجي.

يتطلب تنفيذ الصيانة الوقائية التخطيط الجيد وتحديد الخطوات المطلوبة، ويمكن استخدام برامج إدارة الصيانة لتنظيم الأنشطة وتتبع تاريخ الصيانة والمعلومات الفنية للأنظمة والمعدات.

بشكل عام، تعتبر المراقبة الشبكية أداة أساسية لضمان أمان وكفاءة الشبكات الحاسوبية[6].

9-أهمية استخدام البرامج الحرة في عملية المراقبة والرصد

استخدام البرامج الحرة في عملية المراقبة والرصد له العديد من الفوائد والأهمية، ومنها:

- ✓ **التكلفة:** تعتبر البرامج الحرة أقل تكلفة من البرامج التجارية، حيث يمكن الحصول عليها بشكل مجاني أو بتكلفة منخفضة جدًا.
- ✓ **المرونة:** تتيح البرامج الحرة للمستخدمين إمكانية تعديل البرامج وتكييفها وفقًا لاحتياجاتهم ومتطلباتهم الفردية، وبالتالي توفير مرونة أكبر لعملية المراقبة والرصد.

- ✓ **المجتمع الواسع:** تحظى البرامج الحرة بدعم كبير من قبل مجتمع البرمجيات الحرة والمفتوحة المصدر، مما يساعد على تحسين البرامج وتحديثها بشكل مستمر.
- ✓ **الأمان:**يعتبر استخدام البرامج الحرة أكثر أمانًا بسبب وجود مجتمع يعمل على فحص البرامج وتحديثها وتطويرها بشكل مستمر.
- ✓ **الحرية:**تمنح البرامج الحرة المستخدمين حرية استخدام البرامج وتعديلها وتوزيعها بحرية، وبالتالي تمنحهم حرية التحكم في عملية المراقبة والرصد بشكل أكبر.

بالإضافة إلى ذلك، فإن استخدام البرامج الحرة في عملية المراقبة والرصد يساعد على توفير العديد من الميزات والوظائف المفيدة، مثل التنبيهات الفورية، وتحليل البيانات في الوقت الحقيقي، وتحديد أي عناصر تسبب بطء أو انخفاض في الأداء، وتوفير الحلول السريعة للمشاكل.

10- عملية تحليل الأداء والتحسين في مراقبة الشبكات والرصد

عملية تحليل الأداء والتحسين في مراقبة الشبكات والرصد هي عملية مهمة لتحسين أداء الشبكات وتوفير الوقت والجهد في الصيانة والإصلاح. تشمل هذه العملية عدة خطوات، ومنها:

- ✓ **جمع البيانات:**يتم جمع البيانات المتعلقة بالأداء والاستخدام من أدوات المراقبة والرصد.
- ✓ **تحليل البيانات:**يتم تحليل البيانات المجمعة لتحديد المشكلات والنقاط الضعيفة في الشبكة.
- ✓ **تقييم النتائج:**تُقيّم النتائج المتعلقة بالأداء وتُحدّد المشاكل التي يتطلب العمل عليها.
- ✓ **تصميم الحلول**: يتم تصميم الحلول للمشاكل المحددة، سواء كانت تتعلق بتكوين الشبكة أو تحسين الأداء.
- ✓ **تنفيذ الحلول:** يتم تنفيذ الحلول المصممة وفقًا للتصميم الذي تم إعداده.
- ✓ **مراقبة الأداء:** يتم مراقبة الأداء الجديد للشبكة بعد تنفيذ الحلول الجديدة لتحديد ما إذا كانت تعمل بشكل صحيح أم لا.

تتطلب هذه العملية الخبرة والمعرفة بأدوات المراقبة والرصد، وتوفر عملية تحسين مستمر للشبكة وتحسين أدائها بشكل عام.[5]

خاتمة

بعد دراسة هذا الفصل، يمكن القول بأن مراقبة الشبكة هي عملية حاسمة لإدارة الشبكات بشكل فعال. وبواسطة أدوات مراقبة الشبكة، يمكن للمسؤولين عن الشبكة الحصول على بيانات مفصلة ودقيقة حول حالة الشبكة، وبالتالي التعرف على المشكلات المحتملة قبل أن تتسبب في توقف الشبكة.

كما تم التطرق إلى الأساسيات الهامة لمراقبة الشبكة وأنواع الأدوات المتاحة لهذا الغرض. وتم تقديم أمثلة على بعض الأدوات الشائعة المستخدمة في مراقبة الشبكة مثل برامج الإنذار المبكر، وأدوات مراقبة حركة البيانات، وأدوات مراقبة الأمان.

كما تم التركيز على أهمية إدارة النطاق الترددي والحفاظ على سرعة الشبكة، وتقديم أدوات مفيدة لهذا الغرض. وأخيراً، تم الإشارة إلى أهمية استخدام أدوات الكشف عن الهجمات الإلكترونية وتحسين أمان الشبكة.

في الفصل القادم، سيتم التركيز على تحليل ومراجعة الأدوات المستخدمة في مراقبة الشبكة. وسيتم تقديم نظرة عامة على كيفية تحليل البيانات المنتجة من أدوات مراقبة الشبكة واستخدامها لتحسين أداء الشبكة والحفاظ على سلامتها.

ويتم التركيز في هذه المذكرة على شرح أنواع أدوات المراقبة الشبكية ومميزات كل نوع منها، وكيفية استخدامها للحفاظ على سلامة الشبكة وتحسين أدائها.

الفصل الثاني

تحليل ومراجعة الأدوات المستخدمة في مراقبة الشبكة

الفصل الثاني:تحليل ومراجعة الأدوات المستخدمة في مراقبة الشبكة

مقدمة

في هذا الفصل سنتحدث عن أدوات المراقبة الشبكية التي تعتمد على برامج حرة. يتميز البرنامج الحر بأنه يمنح المستخدم حرية استخدامه وتعديله وتوزيعه وتحسينه، وبالتالي فإن استخدام الأدوات الحرة يعتبر خيارًا جيدًا للمنظمات التي تسعى لتقليل تكاليف التكنولوجيا. ومن بين الأدوات الشهيرة والمستخدمة على نطاق واسع في المراقبة الشبكية هي ناجيوس، وهي أداة توفر ميزات شاملة لمراقبة الشبكات والخوادم والخدمات . بالإضافة إلى ناجيوس ، هناك أيضًا أدوات أخرى مفيدة مثل Zabbix و Icinga و Cacti وغيرها التي سنتحدث عنها في هذا الفصل.

1-عرض أدوات المراقبة والرصد الحرة

تتوفر العديد من أدوات المراقبة والرصد الحرة في السوق، والتي توفر الكثير من المزايا والإمكانيات لمراقبة ورصد شبكات الحاسوب بشكل فعال وبدون تكلفة إضافية. تساعد هذه الأدوات المستخدمين على تحسين أداء الشبكات وتشخيص المشاكل بسرعة وسهولة، وذلك من خلال عرض البيانات والإحصائيات المفصلة وتوفير التحليلات المتقدمة.

وتشمل هذه الأدوات العديد من الخيارات والميزات التي تتضمن مراقبة الأداء ورصد حركة المرور وإدارة الأخطاء والتنبيهات المباشرة والتقارير المفصلة وغيرها الكثير. وبالإضافة إلى ذلك، تتوفر هذه الأدوات بتكلفة منخفضة أو حتى بشكل مجاني، مما يجعلها الخيار الأمثل للمستخدمين الذين يبحثون عن أدوات مراقبة ورصد شبكات الحاسوب بكلفة مناسبة.

ومن بين أمثلة هذه الأدوات الحرة، نذكر أدوات مثل ناجيوس و Zabbix و Cacti و Icinga و Observium وغيرها الكثير، والتي تتميز بالدقة والموثوقية والتعددية في الخيارات والإمكانيات التي توفرها.[7]

2-تعريف ناجيوس

هو برنامج حر ومفتوح المصدر يستخدم كأداة لمراقبة الشبكات وأنظمة الحاسوب. يتيح ناجيوس للمسؤولين عن النظام مراقبة حالة الأجهزة والخوادم والتطبيقات والخدمات الأخرى في الشبكة بشكل دوري وتلقي إشعارات في الوقت الحقيقي عند حدوث مشاكل أو انقطاع في الخدمة[4]

يتميز ناجيوس بالعديد من الميزات المهمة التي تجعله أداة قوية لمراقبة الشبكات، ومن أبرز هذه الميزات:

- **سهولة الاستخدام:**يعتبر ناجيوس سهل الاستخدام والتعلم، حيث يمكن للمستخدمين تثبيته واستخدامه بشكل سريع دون الحاجة لخبرة تقنية كبيرة.
- **قابلية التوسع:**يمكن لمستخدمي ناجيوس توسيع وتخصيص الميزات والوظائف حسب احتياجاتهم، من خلال استخدام الإضافات والمكونات الإضافية.
- **الإشعارات الفورية:**يتميز ناجيوس بالقدرة على إرسال إشعارات فورية عند اكتشاف أي مشكلة في الشبكة، مما يساعد على تجنب حدوث أي توقف في الخدمات المقدمة.
- **مراقبة متعددة البائعين:**يمكن لـ ناجيوس مراقبة أنظمة متعددة البائعين ومتعددة البروتوكولات، مما يجعلها أداة مفيدة للغاية للمؤسسات التي تعتمد على أنظمة وتقنيات متنوعة.
- **تقارير مفصلة:** يوفر ناجيوس تقارير مفصلة حول أداء الشبكة والخوادم والأنظمة، ويساعد في تحديد النقاط الضعيفة والتحسينات الممكنة.
- **الدعم القوي:**يتمتع ناجيوس بدعم قوي من قبل المجتمع المفتوح المصدر والمطورين، ويتم تحديثه وتطويره باستمرار لتلبية احتياجات المستخدمين.

3-خصائص برنامج ناجيوس (Nagios)

- **المراقبة في الوقت الحقيقي:** يتمكن ناجيوس من مراقبة الأنظمة والشبكات في الوقت الحقيقي، مما يسمح برصد الأخطاء والأعطال على الفور واتخاذ الإجراءات اللازمة لإصلاحها قبل أن تؤثر على عمليات الأعمال.[7]
- **القدرة على التخصيص:**يتيح ناجيوس للمستخدمين إمكانية تخصيص وتعديل المراقبة وفقًا لاحتياجاتهم الخاصة وتطبيقاتهم.
- **دعم العديد من البروتوكولات:**يمكن لناجيوس مراقبة العديد من البروتوكولات مثل TCP/IP و SNMP و SSH و SMTP و FTP وغيرها، مما يوفر مرونة وقابلية للتوسع في استخدامه.

- **التنبيهات:**يقوم ناجيوس بإرسال التنبيهات الفورية عند حدوث أي أعطال أو أخطاء في الشبكة أو أنظمة المراقبة، مما يسمح بالتدخل السريع وتجنب توقف الخدمات.
- **التقارير والإحصائيات:**يتيح ناجيوس للمستخدمين إمكانية الحصول على تقارير وإحصائيات مفصلة عن أداء الشبكة وأنظمة المراقبة، مما يساعد في تحسين الأداء وتحديد النقاط التي تحتاج إلى تحسين.
- **دعم الإضافات:**يوفر ناجيوس العديد من الإضافات التي يمكن استخدامها لتحسين وتخصيص المراقبة مثل إضافات التنبيه عبر البريد الإلكتروني أو الرسائل النصية أو إضافات للتحكم عن بعد.
- **دعم المجتمع:**يوفر ناجيوس دعمًا واسعًا من المجتمع العالمي للمستخدمين، مما يساعد في تحسينه

4-الوظائف

تتضمن العديد من الوظائف في ناجيوس، ومن بين الوظائف الأكثر شيوعًا،

يمكننا ذكر ما يلي:

- مراقبة خدمات الشبكات (SMTP, http…) و المضيفين وموارد النظام (CPU , charge mémoire…)
- تحديد حالة الكائنات والموارد اللازمة لتشغيل النظام بشكل تلقائي وعن بعد باستخدام المكونات الإضافية الخاصة به.
- عرض حالات الخدمات والمضيفين بألوان محددة.
- إنتاج التقارير.
- رسم الخرائط للشبكة.
- إدارة التنبيهات.
- مراقبة العمليات (sous Windows, Unix…) .
- مراقبة خدمات الشبكات :

(SMTP, POP3, HTTP, NNTP, ICMP, SNMP, LDAP, etc ...) .

- يمكن استخدام المراقبة عن بعد باستخدام SSH أو tunnel SSL .
- تمت كتابة المكونات الإضافية باستخدام لغات البرمجة الأكثر تلاءما لمهمته :

(Bash, C++, Python, Perl, PHP, C#, etc.)

جميع هذه الميزات يتم ضمانها بفضل إدارة ومراقبة الشبكة ومختلف كياناتها بشكل مركزي. [7]

يقوم **الشكل رقم 1** بنمذجة هذا الجانب:

الشكل رقم 1 يوضح عملية تجميع المعلومات والإشراف الشامل التي يقدمها ناجيوس لشبكة الحوسبة المركزية.

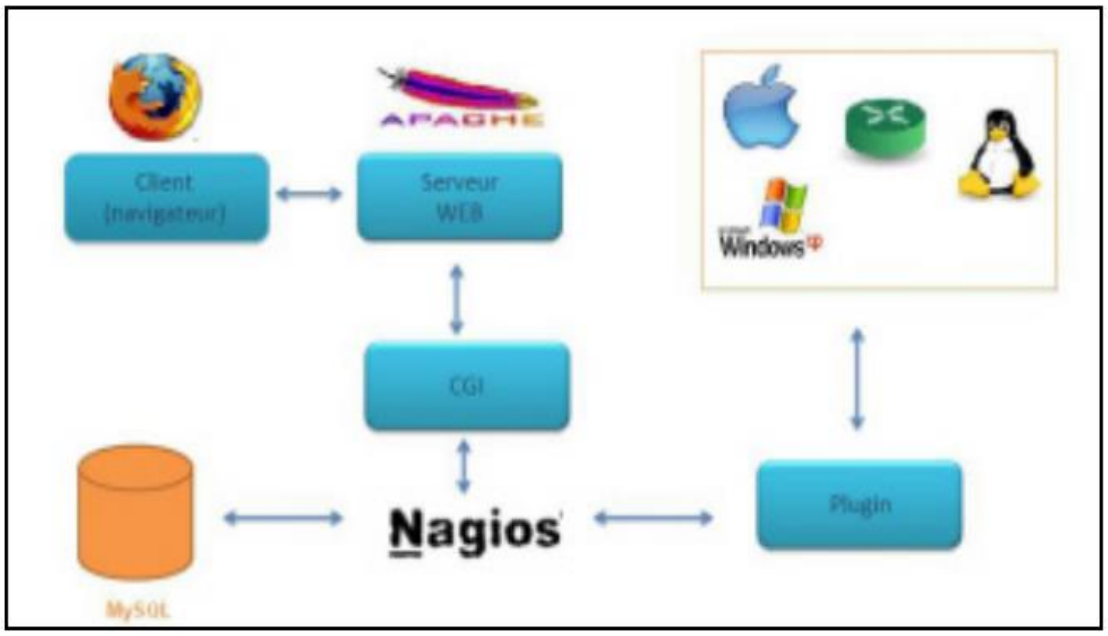
5-تصميم ناجيوس

تعتمد ناجيوس على نموذج خادم-عميل حيث يعمل الخادم كنقطة مركزية لجمع المعلومات بينما تعمل الآلات الأخرى في الشبكة كعملاء مسؤولين عن إرسال المعلومات إلى الخادم. يمكن تقسيم البنية العامة لناجيوس إلى ثلاثة أجزاء تتعاون مع بعضها البعض:

- **النواة :** وهي تعتبر قلب خادم ناجيوس ، تم إطلاقها كبرنامج خفي ومسؤول عن جمع المعلومات وتحليلها والاستجابة والوقاية والإصلاح وجدولة الفحوص (متى وفي أي ترتيب)
وهذا المبدأ يمكنه توزيع عمليات الفحص على أفضل وجه في الوقت المناسب لتجنب الحمل الزائد على الخادم والآلات المراقبة.
- **المنفذون :** هم المكونات الإضافية تأتي بشكل أساسي في النظام ، وهم المسؤولون عن تنفيذ عمليات التحكم والاختبارات على الأجهزة البعيدة أو المحلية وإرجاع النتائج إلى نواة خادم ناجيوس

- **واجهة المستخدم الرسومية (IHM) :**التي تعد واجهة تفاعلية متاحة عبر الويب مصممة لجعل النتائج أكثر قابلية للاستخدام، وتعتمد على واجهات CGI (Common Gateway Interface)التي تترجم الإجابات الخاصة بالمشغلات لعرضها في الواجهة. تستخدم هذه الواجهة لعرض نظرة عامة واضحة على النظام وحالة الخدمات التي يتم مراقبتها وإنشاء التقارير وعرض السجلات. بشكل عام، يمكن للمستخدم تحديد الخدمات أو المضيفين الذين يحتاجون إلى تدخل المسؤول عن طريق النظر في واجهة الاستخدام. يمكن ربط ناجيوس بقاعدة بيانات MySQL اوPostgres [8]

يعرض في الشكل التالي نموذج لتصميم ناجيوس



الشكل رقم 2 تصميم ناجيوس(Nagios)

6-الملحقات (Plugins)

تعد الـ Plugins جزءًا أساسيًا من برنامج ناجيوس، حيث تعمل على تنفيذ المهام المختلفة لجمع المعلومات اللازمة للمراقبة وتحليلها وإعادة تقديم البيانات بشكل صيغة قابلة للفهم والتصور.

ويمكن تعريفها بأنها برامج صغيرة مكتوبة بلغة السكريبت مثل (Bash) أولغات البرمجة المختلفة مثل الـ C والـ Python والـ Perl وغيرها، وتقوم بتحليل حالة النظام وإجراء فحوصات للتأكد من عمل جميع المكونات الحية بشكل صحيح.

وتتيح الـ Plugins إمكانية إجراء فحوصات تختلف في نوعها وطريقة تنفيذها، حيث يمكن استخدامها للتحقق من حالة الـ CPU والـ Memory والـ Disk والـ Network والـ Services وغيرها من المكونات الحيوية للنظام. ويتم تشغيل الـ Plugins بصورة دورية من قبل نواة الناجيوس، وتستخدم لجمع المعلومات وإعداد التقارير وتحديد حالة النظام والإشعار بأي مشكلات قد تحدث.

وتتوفر مجموعة كبيرة من الـ Plugins المجانية والمفتوحة المصدر والتي يمكن تخصيصها لتناسب احتياجات المستخدم، وكذلك يمكن كتابة Plugins مخصصة من قبل المستخدمين للتعامل مع متطلباتهم الخاصة. [7]

الجدول رقم 1 يلخص العلاقة بين نواة الناجيوس والمكونات الإضافية(plugins) ، حيث تتم هذه العلاقة من جهة بواسطة ملفات التكوين التي تعرف الأوامر التي يجب تنفيذها، ومن جهة أخرى بواسطة رمز العودة (code of return) من المكونات الإضافية.

رمز الرجوع	الحالة	المعنى
1	OK	كل شيء جيد
2	Warning	تم تجاوز الحد الطبيعي للخدمة
3	Critical	الخدمة بها مشكلة
4	Unkown	غير قادر على معرفة حالة الخدمة

جدول رقم 1: معاني رموز العودة

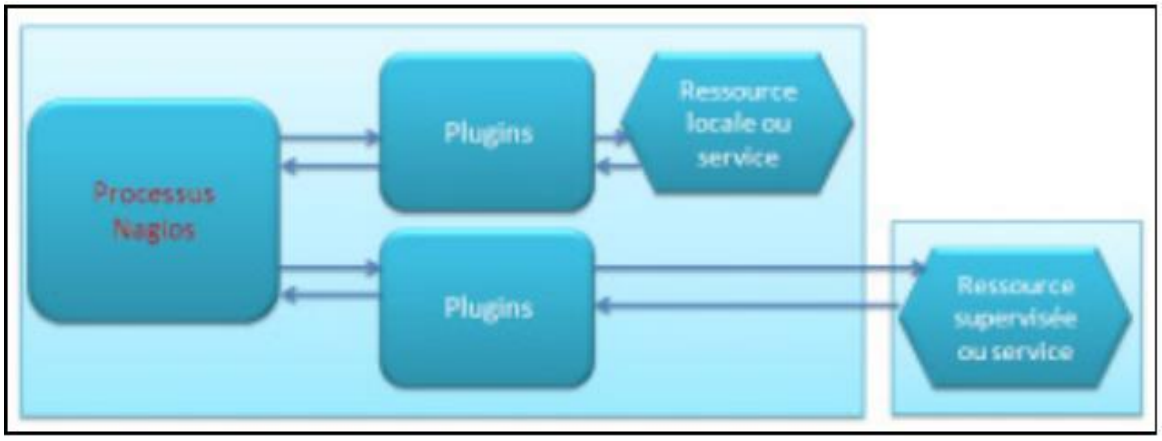
ناجيوس يأتي مع حزمة من الإضافات القياسية التي تضم الأكثر استخداماً. للاستخدام الأساسي والبسيط، يجب أن تكون هذه الإضافات كافية. وفيما يلي بعض الأمثلة عليها:

- check_http يتحقق من وجود خادم ويب.
- check_load يتحقق من تحميل وحدة المعالجة المركزية المحلية.
- check_ping يرسل طلب Ping إلى مضيف.
- check_pop يتحقق من وجود خادم.POP3
- check_procs يعد العمليات المحلية.
- check_smtp يتحقق من وجود خادمSMTP
- check_snmp يرسل طلب SNMP (الممرر كوسيط) إلى المضيف.
- check_ssh يتحقق من وجود خدمةSSH
- check_tcp يتحقق من فتح منفذ TCP (الممرر كوسيط)
- check_users يعد عدد المستخدمين على الجهاز المحلي.

يمكن إنشاء إضافة مخصصة وتوصيلها مع ناجيوس مع احترام اتفاقيات رموز الاستجابة المشروحة سابقًا.

يسمح نشاط المجتمع المفتوح المصدر وخاصة ناجيوس 2 بتوفير عدد كبير من الإضافات .[9]

كما يمكن ملاحظة **الشكل 3**، يمكن أن تعمل الإضافات إما بإجراء اختبارات محلية أو عن بعد عن طريق وسائل مختلفة مثل تثبيت عوامل NRPE أوNSClientأو غيرها.



الشكل 3 مبدأ عمل الإضافات (plugins)

7-الرصد السلبي والنشط

يمكن لـ ناجيوس استخدام طرق مختلفة لجمع المعلومات حول أجهزة الشبكة.هناك طريقة تسمى نشطة وأخرى سلبية. يتم الاعتماد في كل منهما على تشغيل خادم خلفية على الجهاز المراد المراقبة عليه. تجمع هاتان الطريقتان عادة لتحقيق أفضل فعالية في الرصد .

نذكر أنه في أي نظام تشغيل متعدد المهام ، فإن البرنامج الخفي هو برنامج كمبيوتر يعمل في الخلفية ، وليس تحت السيطرة المباشرة للمستخدم.

1 المكونات النشطة NRPE

على العكس من المكونات المحلية (التي تعمل على خادم الجهاز المضيفlocalhost، فيما يتعلق بموارده الخاصة) ، يسمح الوحدة / برنامج (Nagios Remote Plugin Executor) NRPE بتنفيذ ما يسمى بالإضافات النشطة مباشرة على الأجهزة المراد مراقبتها. في هذه الحالة ، يتم طلب تنفيذ المكون الإضافي النشط بمبادرة من جهاز خادم ناجيوس .

الإجراء الداخلي هو كما يلي : يطلب خادم ناجيوس ، عبر عميل NRPE ، تنفيذ المكون الإضافي P على الجهاز M. يتلقى البرنامج الخفي NRPE المستضاف على الجهاز M ، طلب تنفيذ المكون الإضافي P. ثم تنفيذ هذا البرنامج المساعد على الجهاز M. يقوم البرنامج الخفي NRPE لجهاز M بجمع المعلومات بعد تنفيذ المكون الإضافي P ويرسل النتيجة إلى خادم ناجيوس . أخيرا ، يفسر خادم ناجيوس النتائج ويبدأ المعالجة المناسبة.

يستخدم هذا النوع من الإجراءات لتوفير المراقبة عن بعد. ومع ذلك ، سيكون من الضروري فتح منفذ اتصال للسماح ل NRPE بالتواصل مع عملائه واسترداد معلومات الحالة المتعلقة بالأجهزة البعيدة.

كما رأينا للتو ، يتم تشغيل NRPE بمبادرة من خادم ناجيوس . هناك قيود على هذا الوضع من التشغيل. على سبيل المثال ، في حالة قيام الأجهزة بمراقبة ما وراء شبكة آمنة ، فإن NRPE يسمح فقط بالاتصالات الصادرة من هذه الشبكة ، أو إذا كانت العملية المراد مراقبتها تتطلب تكرار تنفيذ قصير جدا. فلن يكون تبادل المعلومات مضمونا ، في هذه الحالة نستخدم ما يسمى الإضافات السلبية. (6)

2 المكونات السلبية NSCA

تعمل NSCA على تنفيذ المكوّنات الإضافية السلبية على أجهزة المراقبة. يتم تشغيل هذه المكوّنات الإضافية بناءً على معايير تم تعريفها مسبقًا على الأجهزة البعيدة. على سبيل المثال ، تجاوز 75٪ من سعة التخزين ، اكتشاف نشاط شبكي غير طبيعي أو مجرد فحوصات دورية تتخذ شكل تحديثات تلقائية .

إجراءات العمل الداخلية كالتالي: يقوم مشغل NSCA على جهاز M بتشغيل تنفيذ المكوّن الإضافيP بعد التحقق من معيار التنشيط. في الواقع ، يتم تشغيل المكوّن الإضافي P على جهازM يقوم مشغل NSCA على جهاز M بجمع المعلومات بعد تنفيذ المكوّن الإضافي P وإرسال النتيجة إلى خادم ناجيوس . في النهاية ، يقوم خادم ناجيوس بتفسير النتائج وتشغيل المعالجة المناسبة .نلاحظ جيدًا في هذه الحالة أن طلب تنفيذ المكون الإضافي ليس من مبادرة خادم ناجيوس ، بل من مبادرة الجهاز البعيد نفسه.

7-ملفات التكوين

تستند ناجيوس إلى مجموعة من ملفات تكوين النصوص المختلفة لبناء بنيتها التحتية للمراقبة. سنذكر ونعرف الآن أهم هذه الملفات:

- **Nagios.cfg:** هو الملف الرئيسي لتكوين ناجيوس. يحتوي على قائمة بالملفات الأخرى للتكوين ويتضمن مجموعة من التوجيهات العامة للعمل.

- **Cgi.cfg**: يحتوي على عدد من التوجيهات التي تؤثر على طريقة عملCGI . قد يكون من المثير للاهتمام تحديد التفضيلات المتعلقة بواجهة ويب ناجيوس.
- **Resource.cfg:**يسمح بتحديد المتغيرات العامة القابلة لإعادة الاستخدام في الملفات الأخرى. يمكن استخدام هذا الملف لتخزين معلومات التكوين الحساسة ، حيث لا يمكن الوصول إليه من CGIالتي تولد الواجهة.
- **Commands.cfg:** يحتوي على تعريفات الأوامر الخارجية ، مثل تلك التي ستكون مفيدة لتنبيه المراقبة.
- **Checkcommands.cfg**: يحتوي على تعريفات أوامر التحقق المحددة مسبقًا وتلك المعرفة من قبل المستخدم.
- **Hosts.cfg:** يحدد المضيفين المختلفين في الشبكة الذين يجب مراقبتهم. يتم تعيين اسم الضيف وعنوان IP والاختبار لتحديد حالة الضيف ، وما إلى ذلك لكل ضيف.
- **Services.cfg**: يربط بين كل مضيف أو مجموعة من المضيفين ومجموعة الخدمات التي يجب التحقق منها.
- **Hostsgroups.cfg:** يقوم بتجميع المضيفين في مجموعات بناءً على سمات مشتركة. يمكن لكل مضيف أن ينتمي إلى العديد من المجموعات.
- **Contacts.cfg:** يعلن عن جهات الاتصال التي يجب إعلامها في حالة الحدوث ويحدد إعدادات التنبيهات[7]

خاتمة

في هذا الفصل، تم التركيز على تحليل ومراجعة الأدوات المستخدمة في مراقبة الشبكة، حيث تم استعراض عدد من الحلول والأدوات المتاحة لمراقبة الشبكات، وتم التركيز على الحلول مفتوحة المصدر. و بشكل خاص تم التركيز على أداة ناجيوس ، حيث تم استعراض مزاياها وعيوبها وطريقة عملها وتكوينها.

بعد هذا الفصل، نستطيع أن نستنتج أن هناك العديد من الأدوات والحلول المختلفة المتاحة لمراقبة الشبكات، ويجب علينا اختيار الأداة المناسبة لاحتياجاتنا الخاصة. كما أنه من المهم التأكد من أن الأداة المختارة تلبي الاحتياجات الأساسية للمراقبة، وتتمتع بمزايا القابلية للتخصيص والتوافق مع البنية التحتية للشبكة.

في الفصل القادم، سننتقل إلى تحليل البيانات حيث سنتعلم كيفية جمع وتحليل البيانات من أدوات المراقبة وتقديمها بشكل فعال لاتخاذ القرارات الملائمة. سيتم التركيز على المفاهيم الأساسية لتحليل البيانات وكيفية استخدامها للتحكم في أداء الشبكة وتحسينها.

الفصل الثالث

تطبيق أداء شبكة الناجيوس باستخدام أدوات المراقبة والإشعارات

الفصل الثالث : تطبيق أداء شبكة الناجيوس باستخدام أدوات المراقبة والإشعارات

مقدمة

يتضمن هذا الفصل تطبيق أداء نظام ناجيوس باستخدام أدوات المراقبة والإشعارات.

كما يستكمل الجانب التطبيقي لنظام ناجيوس، حيث سنركز على استخدام أدوات المراقبة والإشعارات لتحسين أداء النظام وتعزيز فعالية الإدارة. سنبدأ بتثبيت ناجيوس وإعداده للعمل كنظام مراقبة مركزي. سنستخدم أدوات المراقبة المختلفة لمراقبة الخوادم والشبكات، بما في ذلك الاختبارات اليدوية والتلقائية والتنبيهات والإشعارات.

كما سيتم تقديم مثال تطبيقي حي لكيفية استخدام نظام ناجيوس لمراقبة خادم محدد. سنستخدم أدوات المراقبة المتاحة في ناجيوس للكشف عن المشاكل في الخادم وإرسال التنبيهات إلى الفريق المعني بالصيانة عند الحاجة. كما سنوضح كيفية تحليل البيانات التي تم جمعها وكيفية استخدامها لتحسين الأداء العام للنظام.

في النهاية، سيتم استخدام هذه الأدوات والإجراءات للحفاظ على تشغيل النظام بشكل مستمر وتحسين أداء الخوادم والشبكات، مما يساعد على تحقيق أهداف العمل وتحسين تجربة المستخدم.

1- La virtualisation

1-1 تعريفه:

هو مجموعة من التقنيات و الأجهزة والبرمجيات التي تسمح بتوفير مجموعة أو مجموعة فرعية من موارد الحاسوب بحيث يمكن استخدامها بمزايا مستقلة عن منصة الأجهزة (التكوين، الموقع).

وهو عبارة عن تقنية تسمح بتشغيل عدة أنظمة تشغيل أو تطبيقات مختلفة على نفس الجهاز، بشكل منفصل عن بعضها البعض، كما لو كانت تعمل على أجهزة فعلية مختلفة.

تتمثل فكرة **virtualisation** في فصل الموارد المادية (الخوادم والحواسيب) عن الموارد البرمجية (أنظمة التشغيل، التطبيقات).

حاليًا، يتم التمييز بين ثلاثة أشكال:

- **Virtualisation** الخوادم
- **Virtualisation** محطة العمل
- **Virtualisation**التطبيقات[4]

1- 2 ما هو الخادم الافتراضي؟

الخادم الافتراضي هو حاوية برمجية معزولة تمامًا وقادرة على إدارة أنظمتها الخاصة وتطبيقاتها كما لو كانت جهاز كمبيوتر فيزيائي باستخدام تقنيات الافتراض. يتصرف الخادم الافتراضي تمامًا كجهاز كمبيوتر فيزيائي ويحتوي على وحدة معالجة مركزية افتراضية خاصة به وذاكرة عشوائية افتراضية وقرص صلب افتراضي وبطاقة الشبكة. لا يمكن لنظام التشغيل التمييز بين الخادم الافتراضي والخادم الفعلي. بالتالي، يوفر الجهاز الافتراضي العديد من المزايا مقارنة بالأجهزة الفعلية :

- **التوافق:** تتوافق الخوادم الافتراضية مع جميع معايير x86 وغيرها .
- **العزلة:** يتم عزل الخوادم الافتراضية عن الآلات الأخرى كما لو كانت آلات فيزيائية .
- **الاستقلالية عن الأجهزة :** تعمل الخوادم الافتراضية بشكل مستقل عن الأجهزة المتعلقة[4] .

1- 3 برنامج Virtual box

لإنشاء بيئات افتراضية تمكن المستخدمين من تشغيل أنظمة التشغيل المختلفة على نفس الجهاز. ونظرًا لزيادة استخدام التقنيات الافتراضية، فإن **Virtual box** يجد مكانًا في العديد من الأجهزة الشخصية. ومع ذلك، تبقى الحالات التي تتطلب تطبيق الإفتراضيات على خوادم الإنتاج المرئية على الإنترنت قليلة الحدوث.

وعلى الرغم من أن برنامج**Virtual box**هو أصغر بكثير من بعض المنافسين مثلVMware، إلا أن شركة Sun استطاعت اللحاق بالمنافسين وتقديم برنامج يعمل بنفس الكفاءة تحت أنظمة التشغيل Macو Windows وأيضًا تحت Linux(GNU/Linux وOpen BSDو FreeBSD)

وهو موضوع عملنا في تهيئة شبكتنا الافتراضية، التي تتكون من انظمة تشغيل مختلفة (Windows،Ubuntu) وذلك بتجربة ناجيوس علي مراقبة ادائها،كما قمنا بتثبيت عدد من الأدوات الإضافية وإعداد الإشعارات للحصول على تنبيهات عند وجود مشاكل لديها .[4]

2-شرح كيفية تثبيت Ubuntuعلي Virtual box

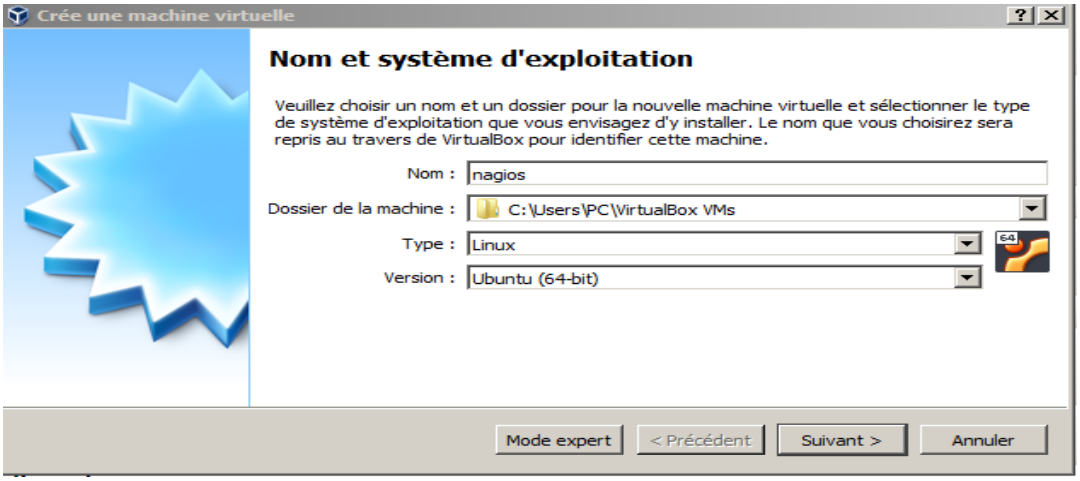
تثبيت نظام تشغيل Ubuntu على برنامج**Virtual Box**يعتبر خطوة مهمة للعديد من الأسباب، مثل اختبار تطبيقات جديدة، أو العمل على بيئة افتراضية لتجنب تأثير أي تغييرات على جهاز الحاسوب الحقيقي، أو حتى للتعلم والتدريب على نظام تشغيل Linux.

في هذا الشرح، سوف نشرح كيفية تثبيت نظام Ubuntu على برنامج**Virtual Box**:

- قم بتنزيل ملف ISO لنظام Ubuntu من الموقع الرسمي :

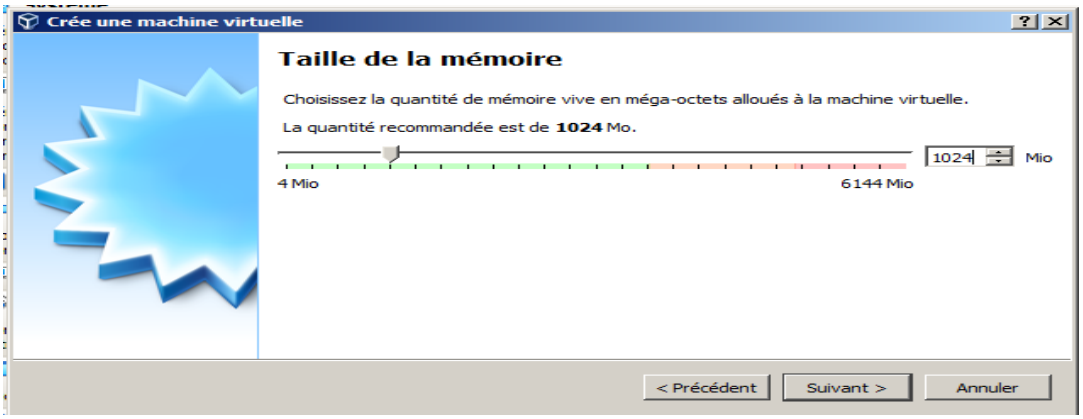
https://releases.ubuntu.com/22.10/ubuntu-22.10-desktop-amd64.iso

- قم بفتح برنامج**Virtual Box**وانقر على "New" لإنشاء جهاز افتراضي جديد.
- اختر اسمًا للجهاز الافتراضي وحدد نظام التشغيل "**Linux**" والإصدار"**Ubuntu**" من القائمة.



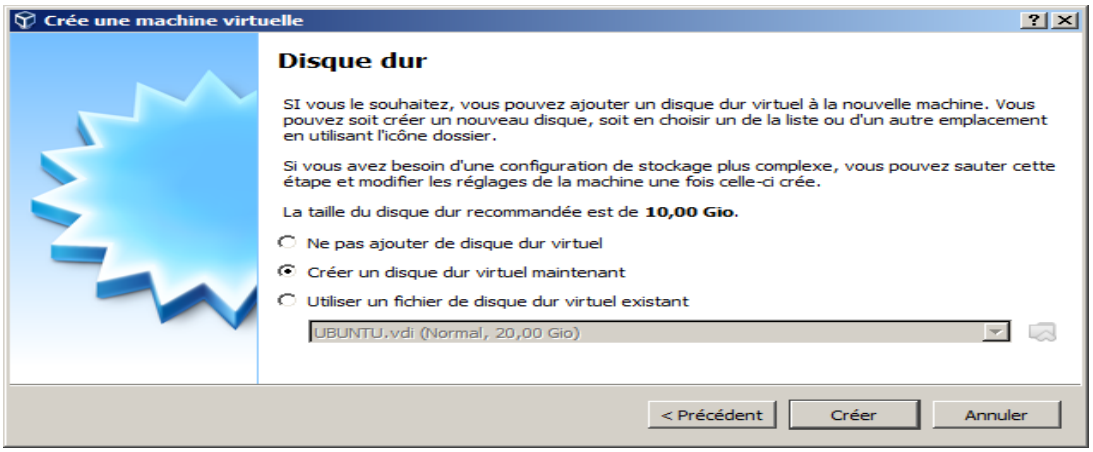
الشكل رقم 4 : إنشاء جهاز افتراضي " Ubuntu"

- قم بتحديد حجم الذاكرة العشوائية (RAM) التي ترغب في تخصيصها للجهاز الافتراضي



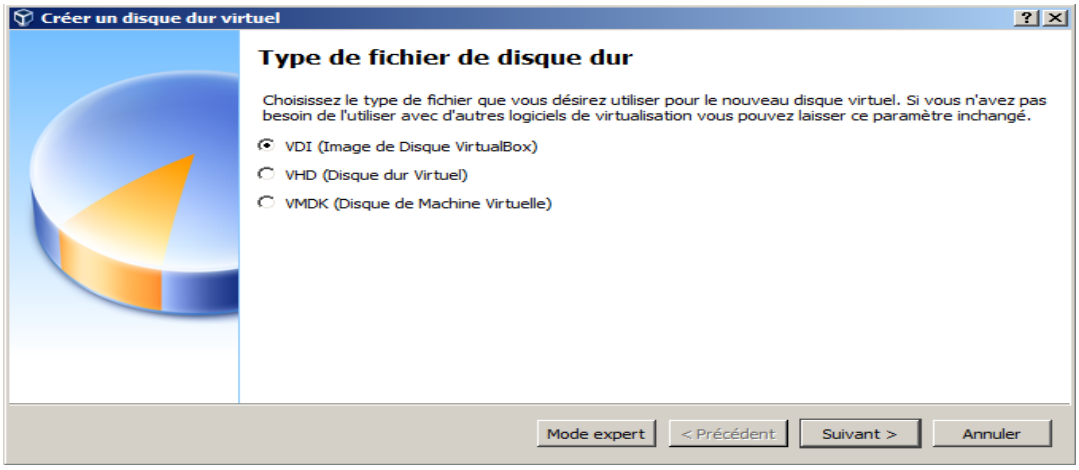
الشكل رقم 5 تحديد حجم الذاكرة

- قم بإنشاء قرص ثابت جديد لتخزين بيانات Ubuntu عليه.
- اختر "Créer un disque dur virtuel maintenant" وانقر على " Créer" .



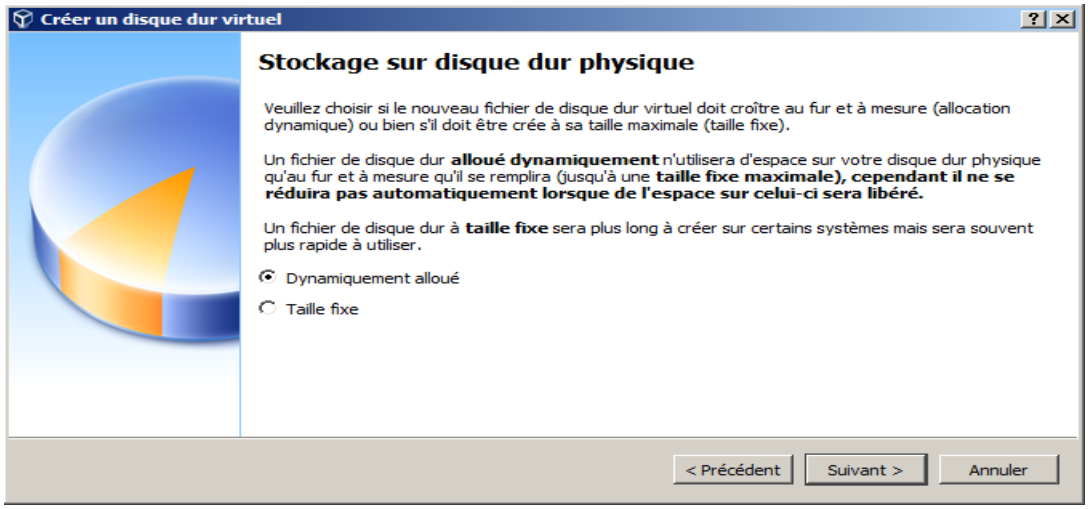
الشكل رقم 6 إنشاء قرص صلب افتراضي

- اختر نوع القرص الثابت الذي تريد استخدامه يفضل VDI وانقر على"Suivant" .



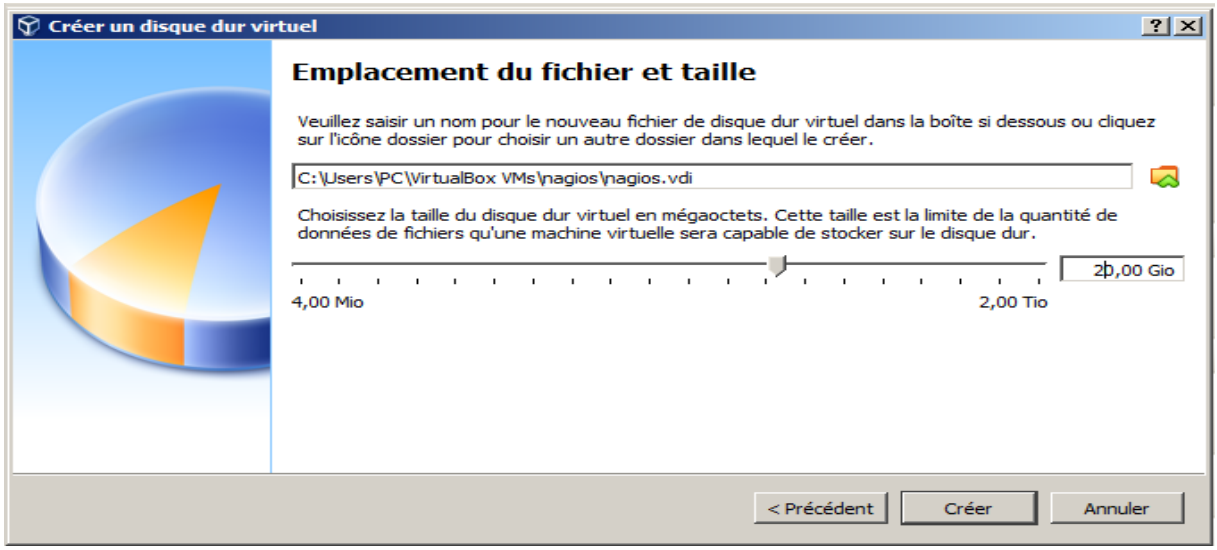
الشكل رقم 7 اختيار نوع القرص

- اختر "Dynamiquement alloué" إذا كنت تريد أن تتمكن من زيادة حجم القرص الثابت فيما بعد عند الحاجة، ثم انقر على."Suivant"



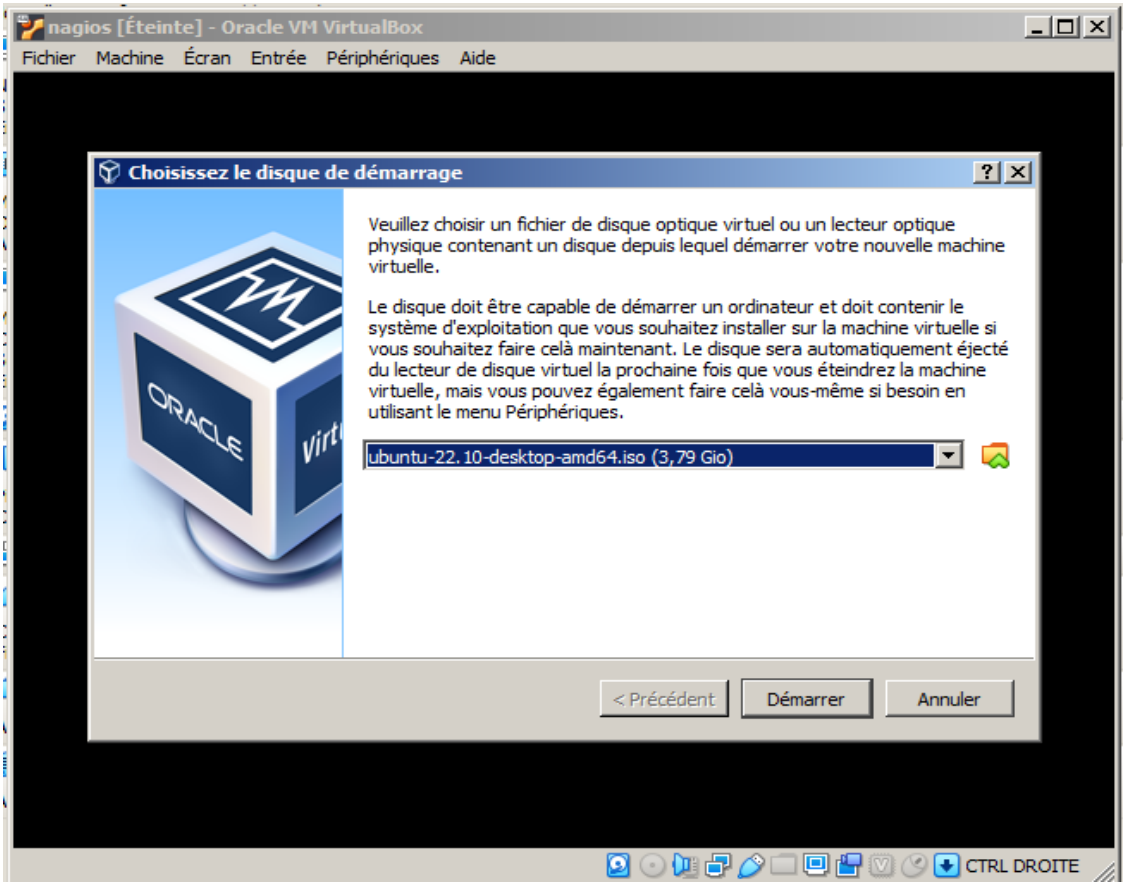
الشكل رقم 8 اختيار زيادة حجم القرص الثابت

- حدد حجم القرص الثابت الذي تريد استخدامه لتثبيتUbuntu ، ثم انقر على« Créer »



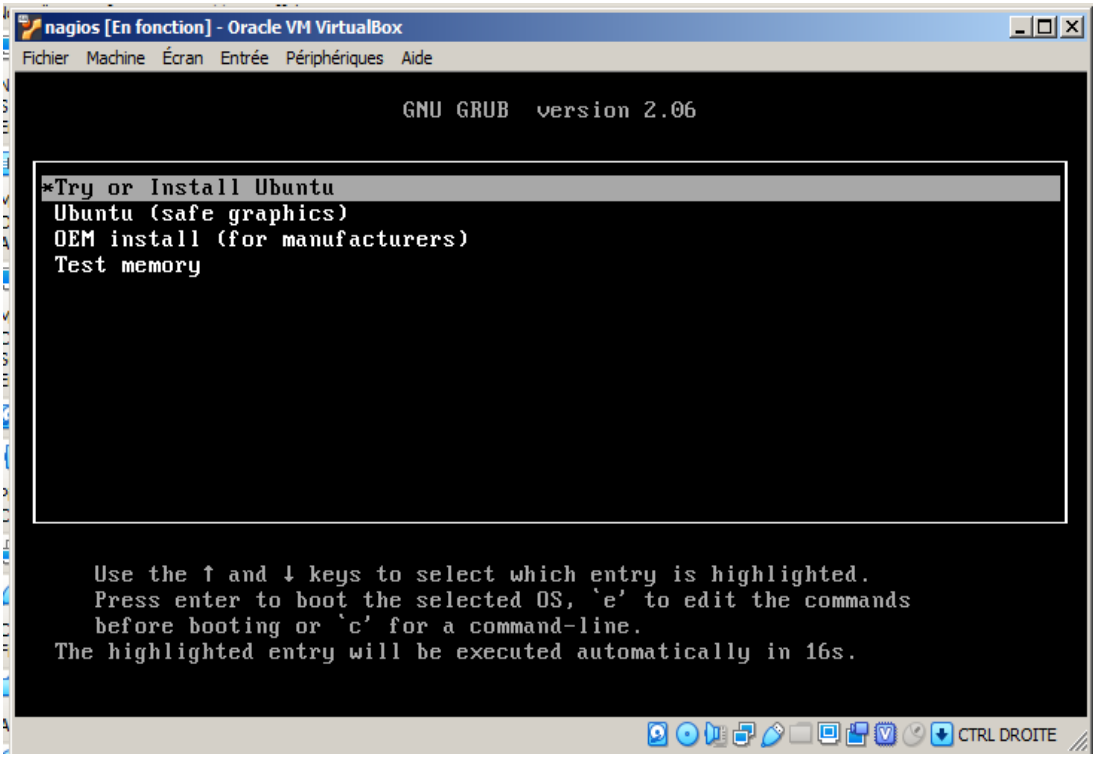
الشكل رقم 9 اختيار حجم القرص الثابت

- بمجرد الانتهاء من الإعدادات، يمكنك تشغيل الجهاز الافتراضي الجديد وتحديد ملف ISO الذي تم تنزيله في الخطوة الأولى كمصدر للتثبيت.

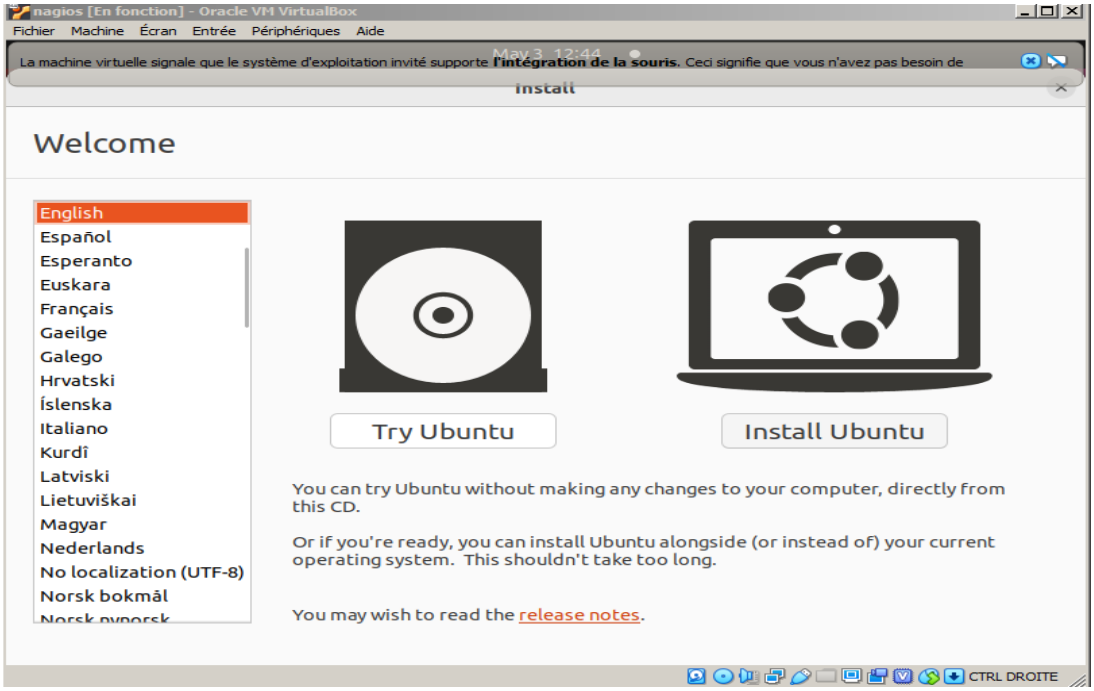


الشكل رقم 10 مصدر التنزيل

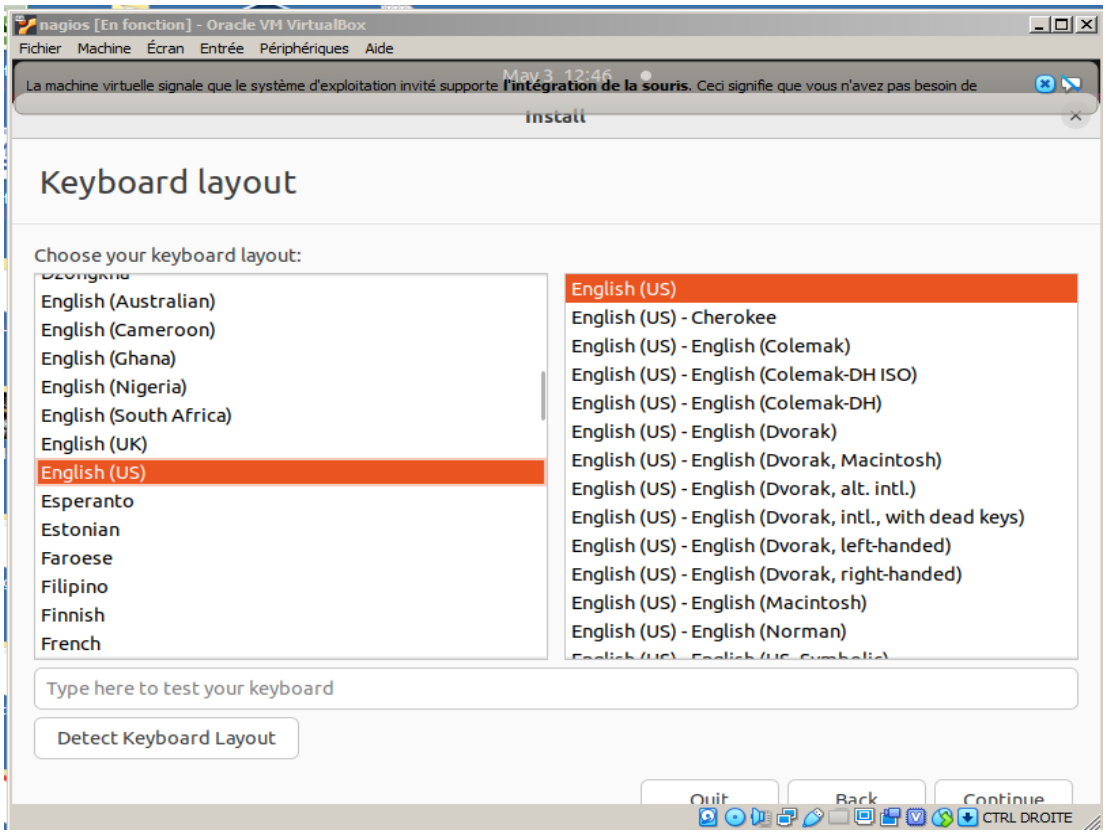
- سيتم تثبيت Ubuntu .



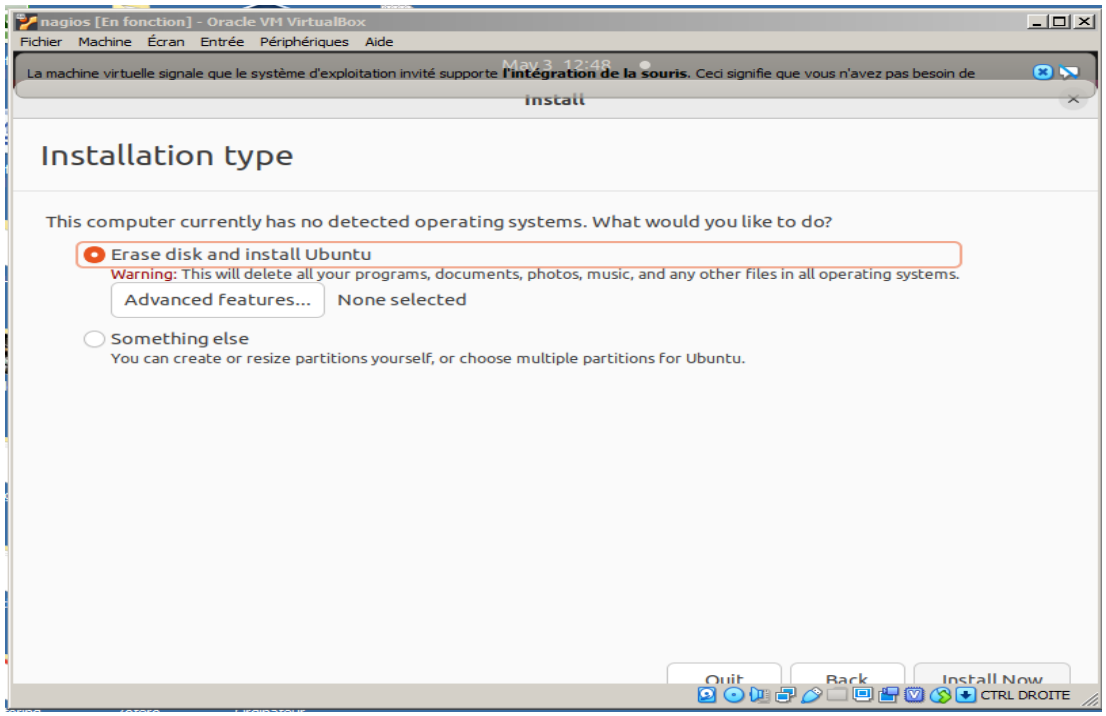
الشكل رقم 11 بداية التثبيت



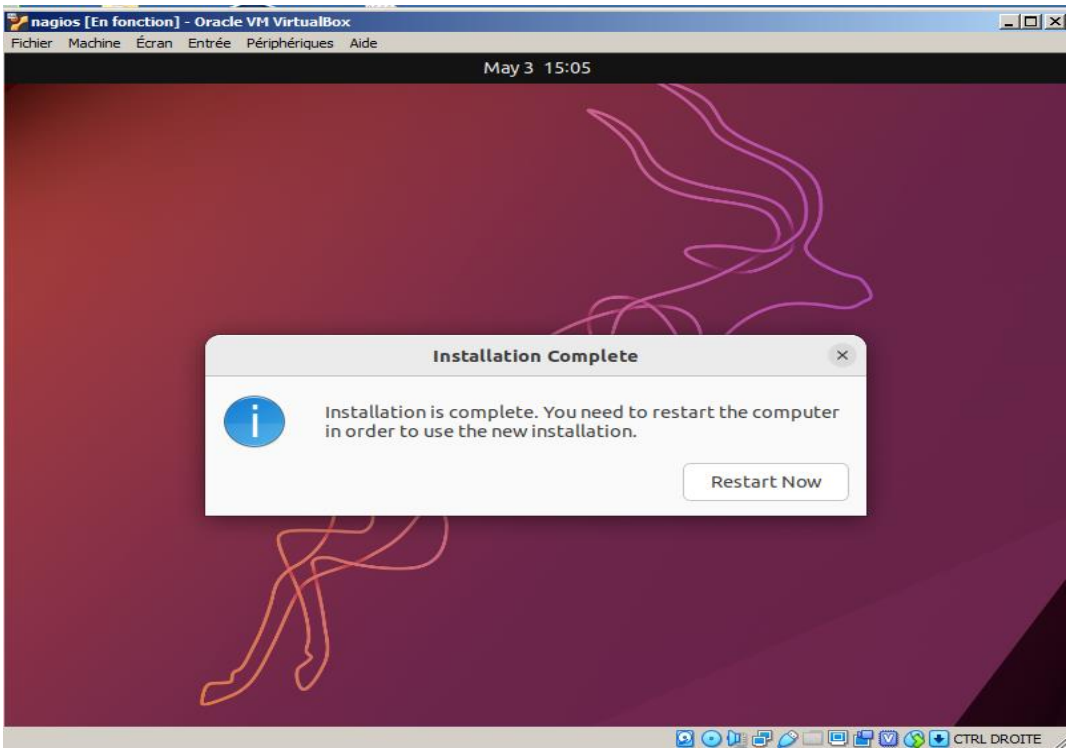
الشكل رقم 12 تثبيتUbuntu



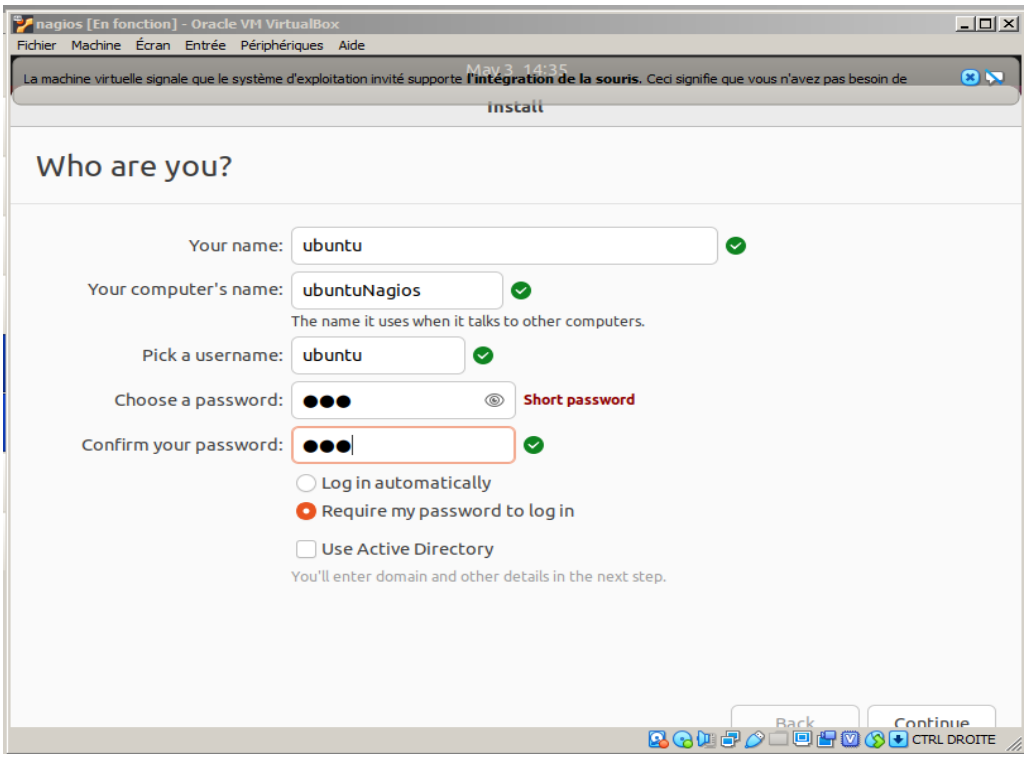
الشكل رقم 13 اختيار اللغة



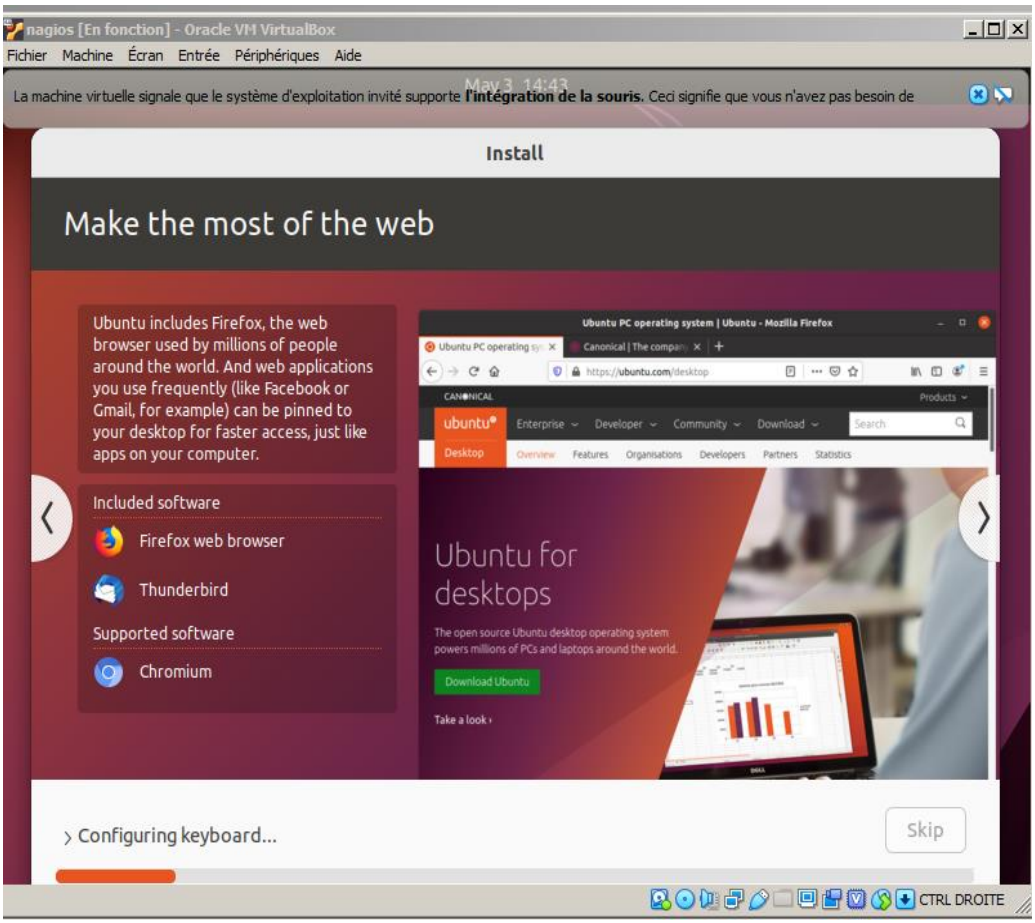
الشكل رقم 14 اختيارات التثبيت



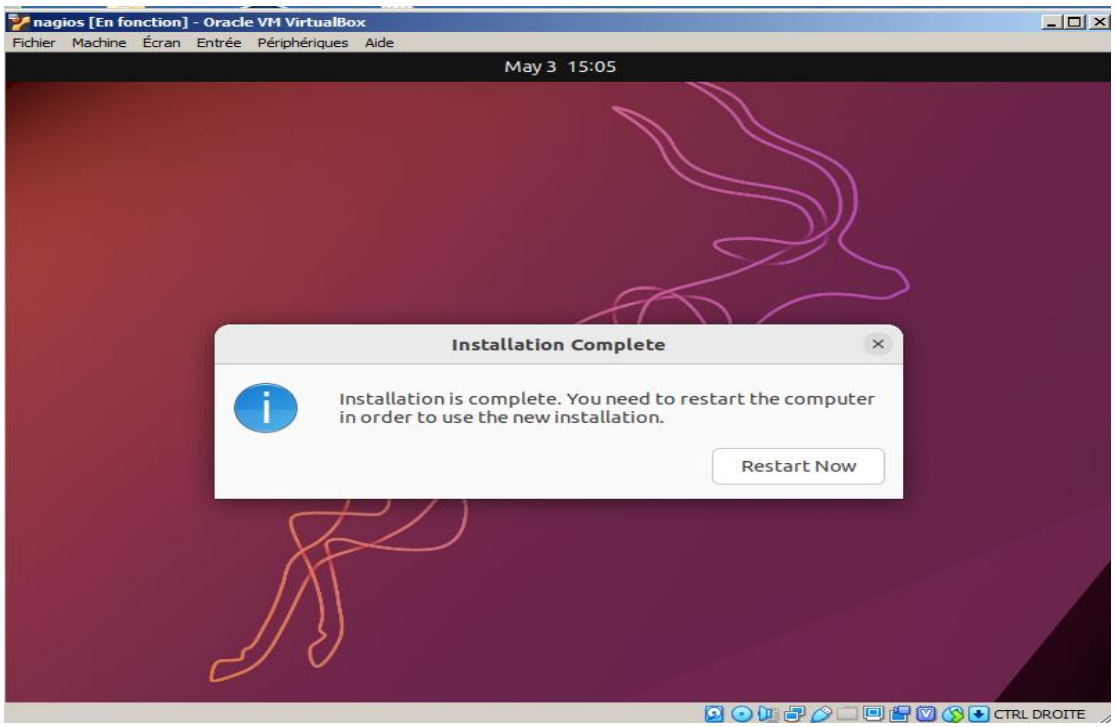
الشكل رقم 15 نهاية التثبيت



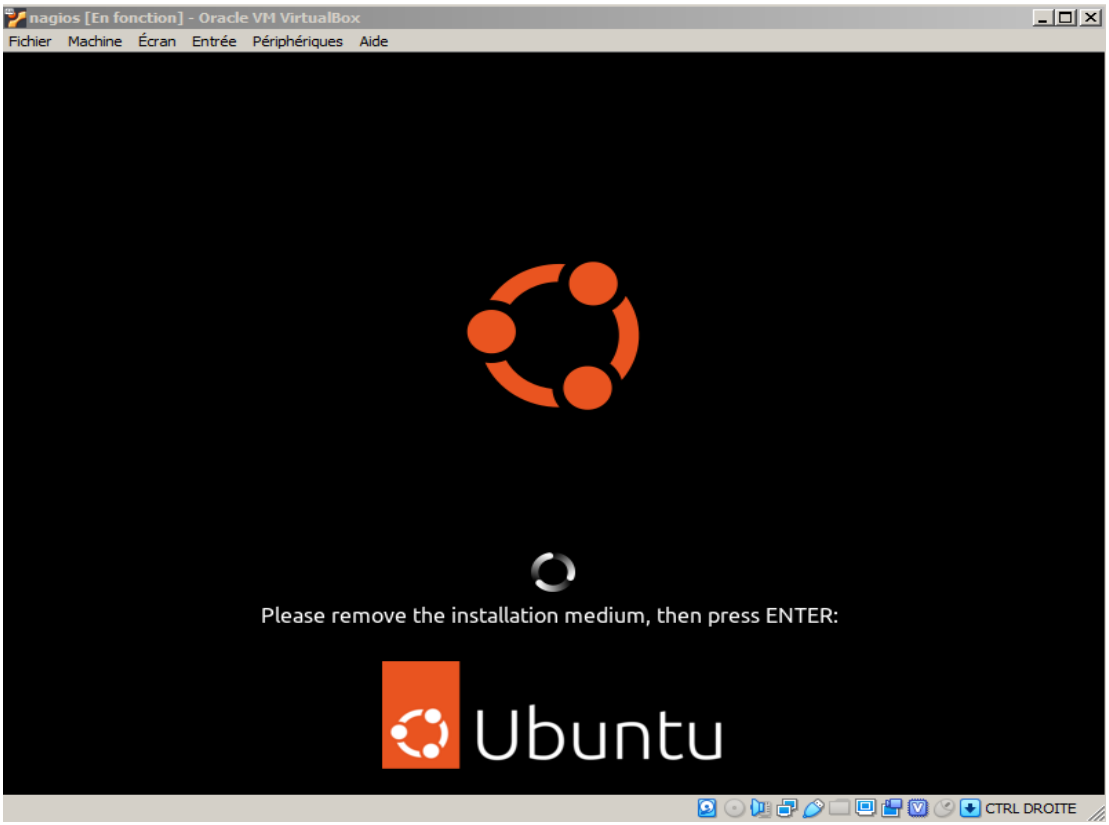
الشكل رقم 16 التسمية وإضافة كلمة السر



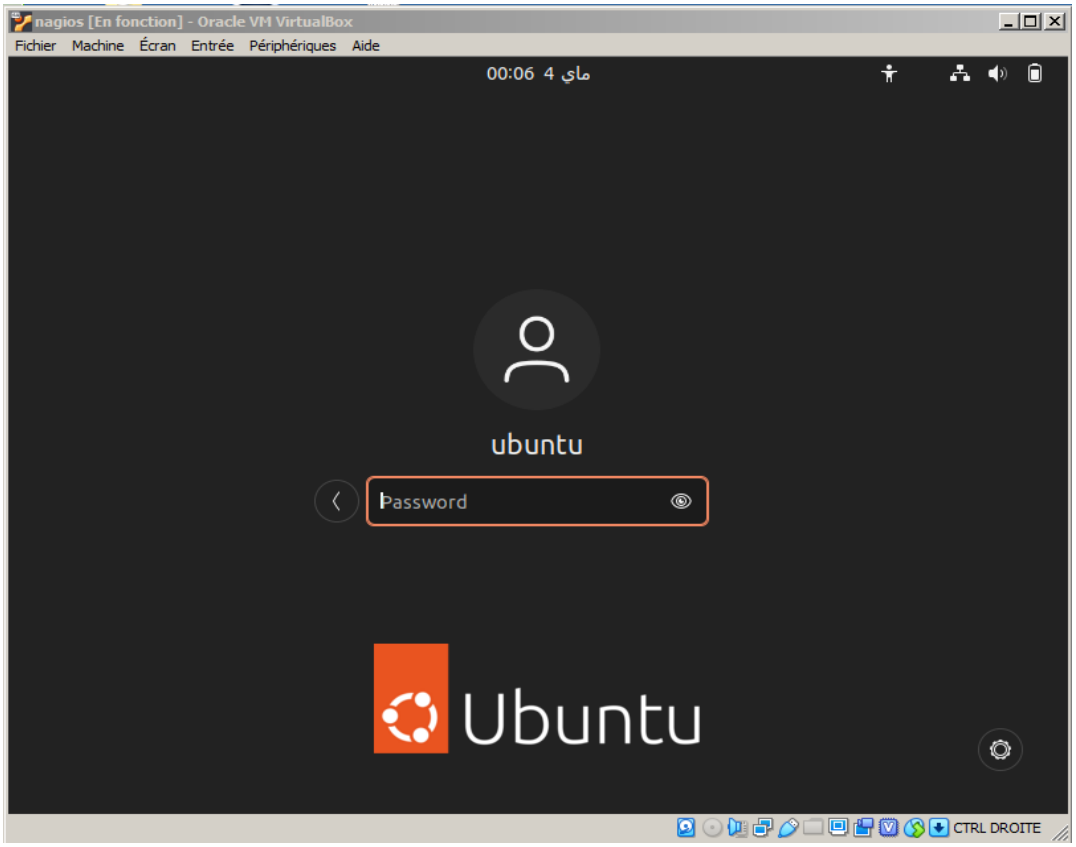
الشكل رقم 17 التثبيت



الشكل رقم 18 إعادة تشغيل الجهاز



الشكل رقم 19 الدخول



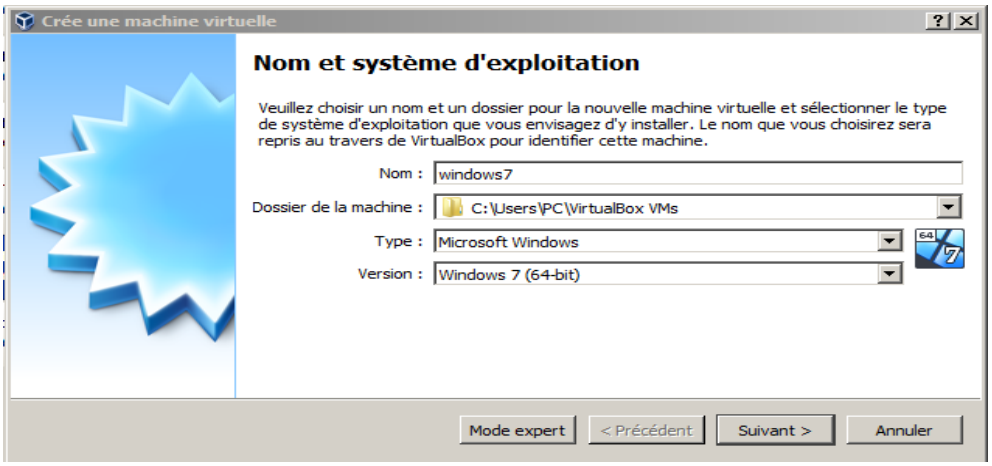
الشكل رقم 20 إدخال كلمة السر

- بعد الانتهاء من التثبيت، يمكن الآن تشغيل Ubuntu على VirtualBox والبدء في استخدامها كنظام تشغيل طبيعي.

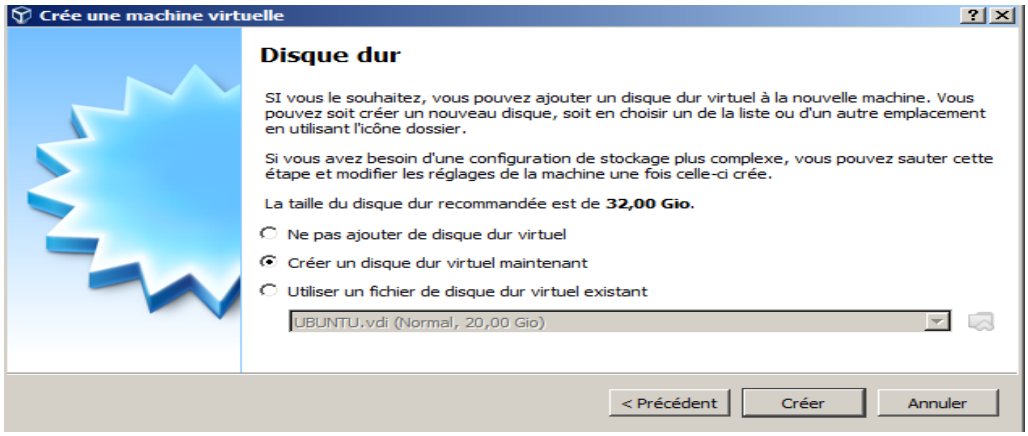
3-شرح كيفية تثبيت Windows علي Virtual Box

يمكن استخدام برنامج **Virtual Box** لتثبيت نظام **Windows** على جهاز الكمبيوتر كنظام ضيف (Guest System) ويتطلب ذلك تحميل نسخة من ويندوز وتوفر مساحة كافية على القرص الصلب لتثبيته كنظام ضيف. يمكنك إتباع الخطوات التالية لتثبيت **Windows** على **Virtual Box** :

- تحميل وتثبيت برنامج Virtual Box على جهاز الكمبيوتر الخاص بك من الموقع الرسمي للبرنامج.
- تحميل ملف ISO لنظام Windows الذي ترغب في تثبيته على **Virtual Box**.
- إنشاء ما يسمى بـ "**Virtual Machine**" في **Virtual Box** وتحديد نوع النظام الضيف وحجم الذاكرة والمساحة الخاصة بالقرص الصلب.

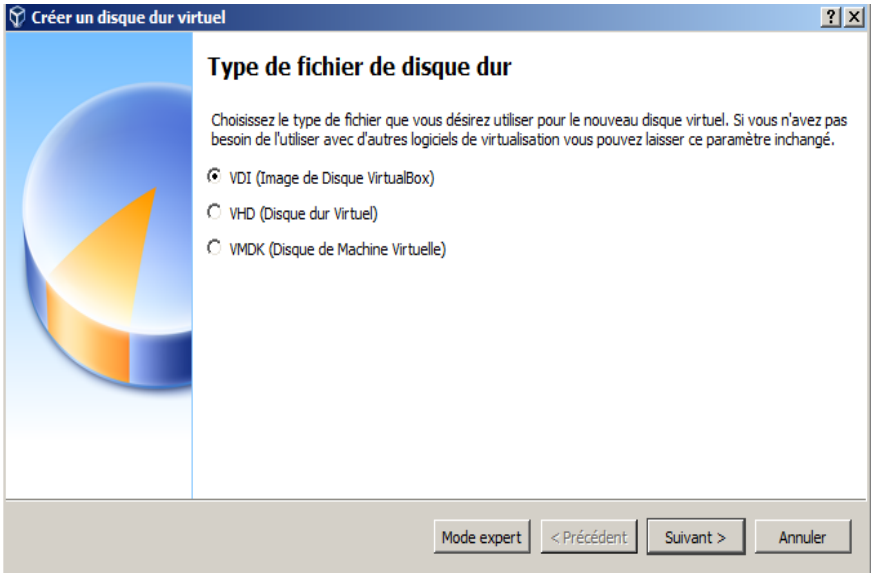


الشكل رقم 21 إنشاء جهاز افتراضي Windows

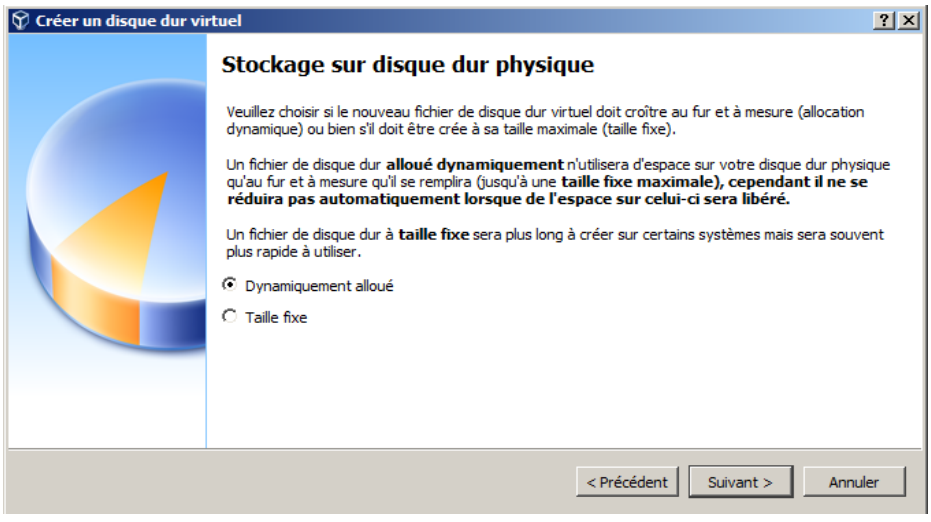


➢ **الشكل رقم 22 إنشاء قرص صلب افتراضي**

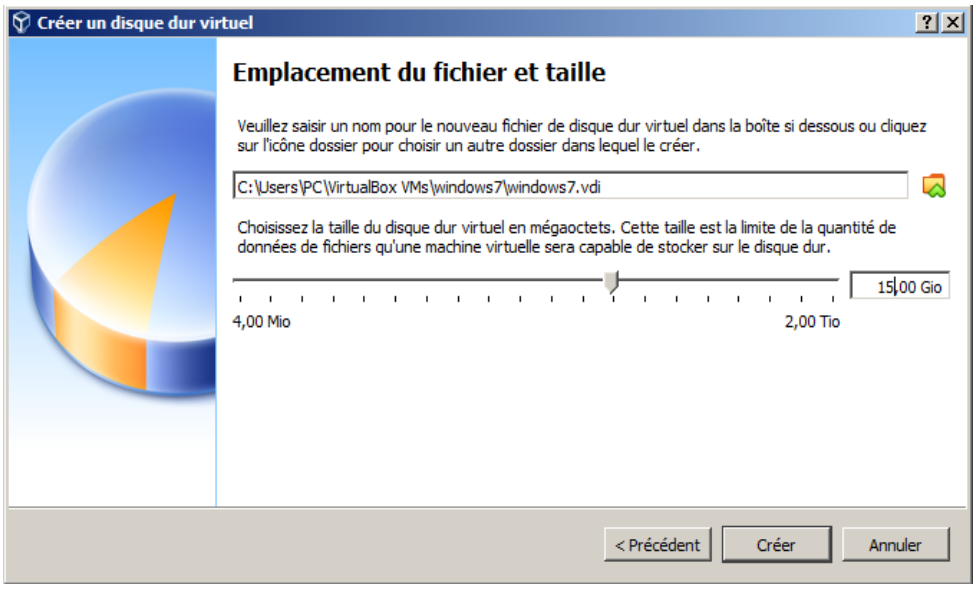
➢ تعيين ملف ISO لنظام Windows كـ "Virtual Optical Disk" لتشغيل النظام.



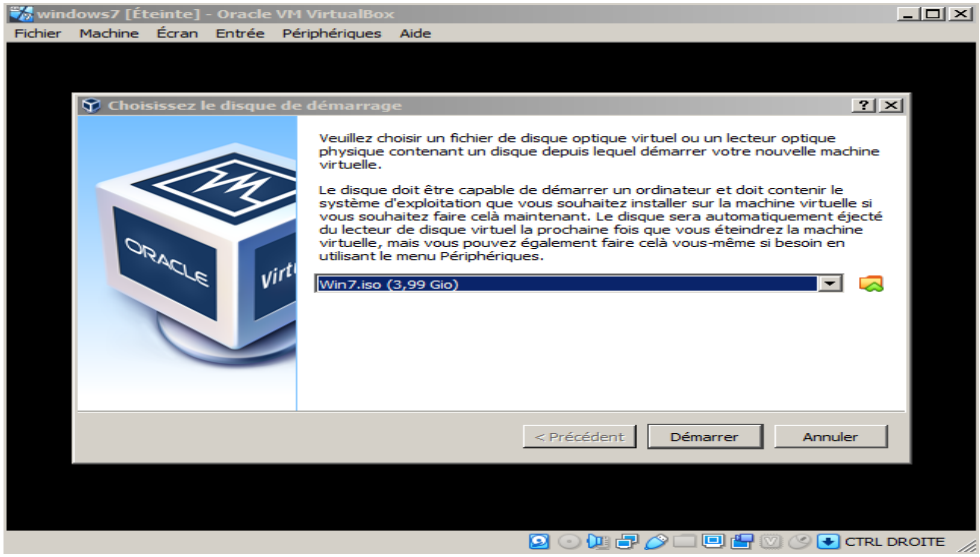
الشكل رقم 23 اختيار نوع القرص



الشكل رقم 24 اختيار زيادة حجم القرص



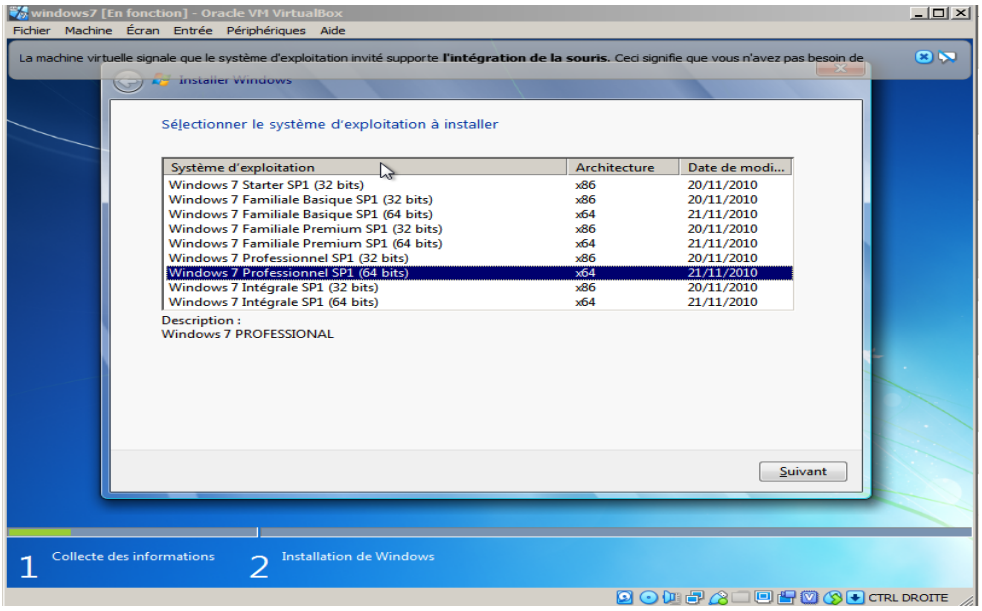
الشكل رقم 25 اختيار حجم القرص



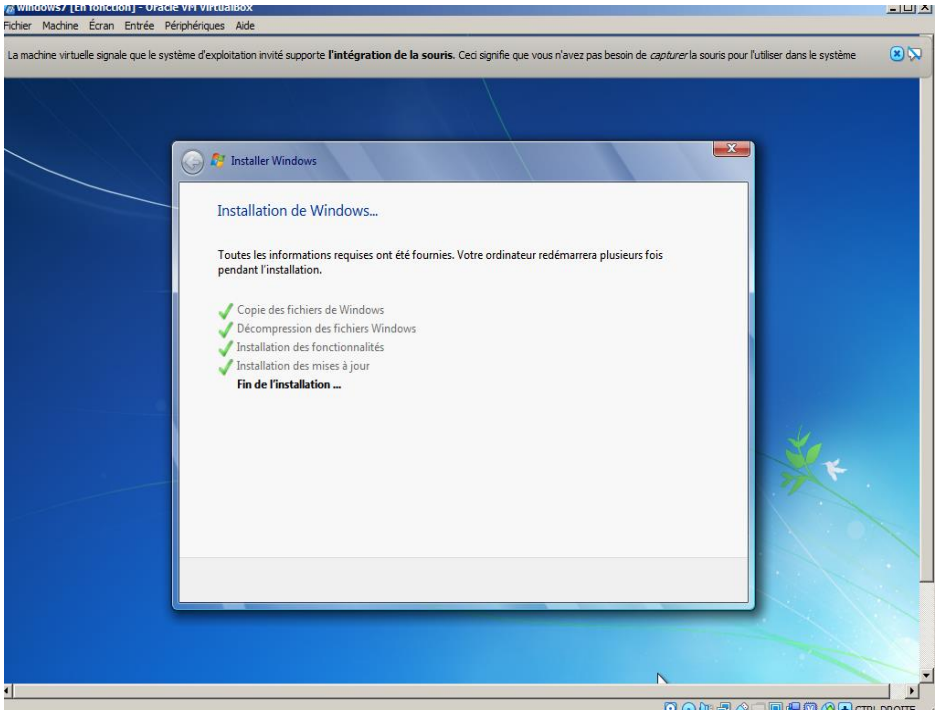
الشكل رقم 26 اختيار ISO Windows 7

الشكل رقم 27 اختيار اللغة

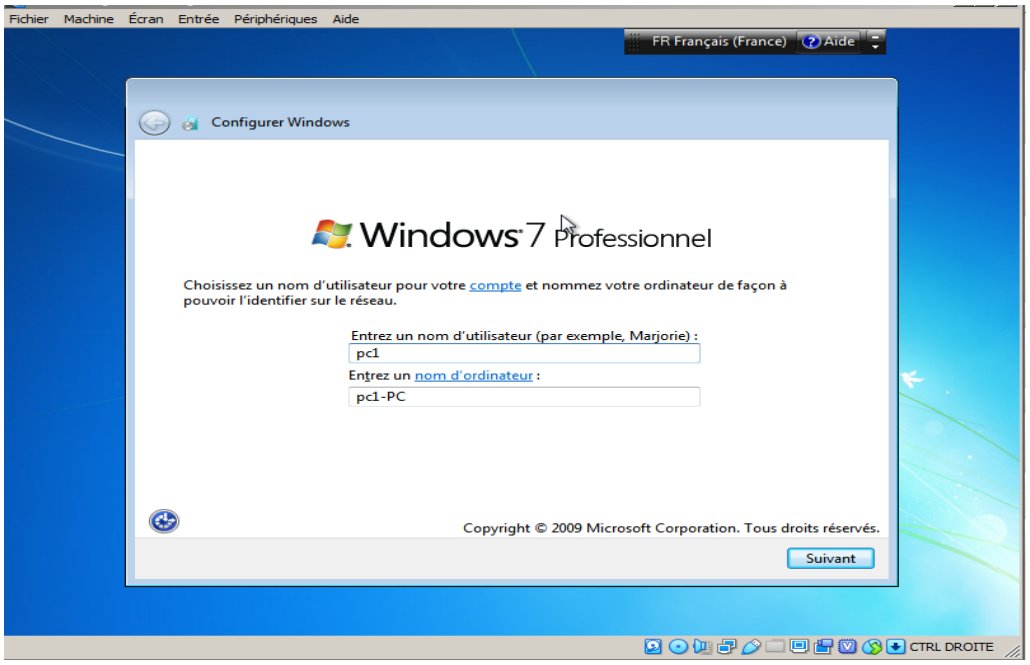
الشكل رقم 28 بداية التثبيت



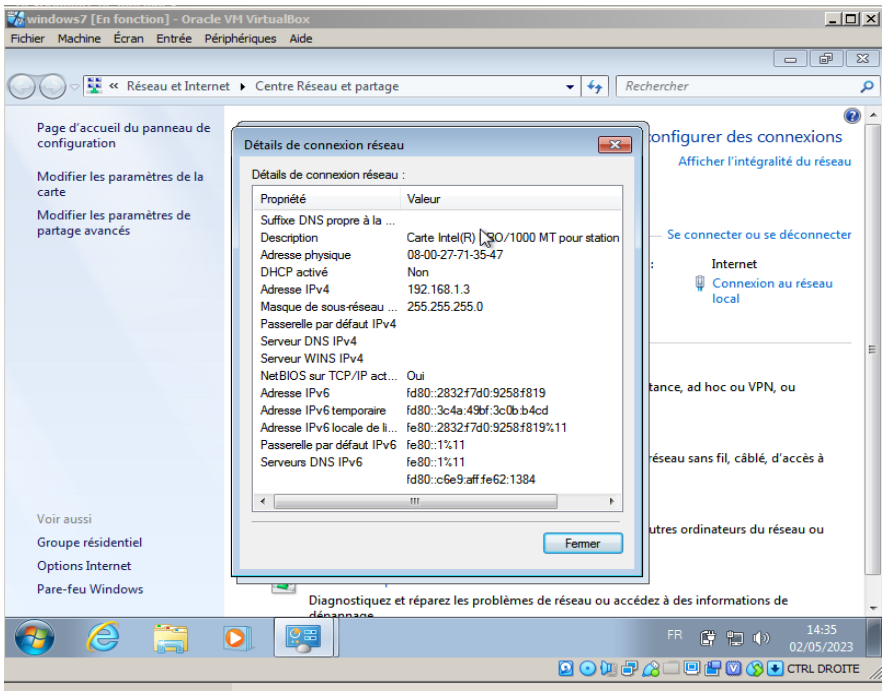
الشكل رقم 29 الاختيار نوع النظام



الشكل رقم 30 نهاية التثبيت



الشكل رقم 31 اسم المستخدم



الشكل رقم 32 بعد تعديل ال Adresse ip

- وبعد ذلك يمكن استخدام **Windows** كنظام مضيف لناجيوس .

4-شرح كيفية تثبيت وإعداد برنامج الناجيوس على نظام Ubuntu

تثبيت برنامج الناجيوس على نظام Ubuntu هو عملية مهمة لإعداد بيئة المراقبة والرصد للشبكة. يتطلب هذا الأمر بعض الخطوات التي يجب إتباعها بدقة لضمان نجاح العملية. سنحتاج إلى تثبيت حزمة Apacheو MySQL و PHP لضمان أن الناجيوس يعمل بشكل صحيح. بعد ذلك، يتم تنزيل برنامج الناجيوس وتثبيته على النظام.

يمكن تثبيت برنامج الناجيوس على نظام Ubuntu بإتباع الخطوات التالية:

- أولا سنقوم بتحديث قائمة الحزم و تثبيت الحزم المطلوبة

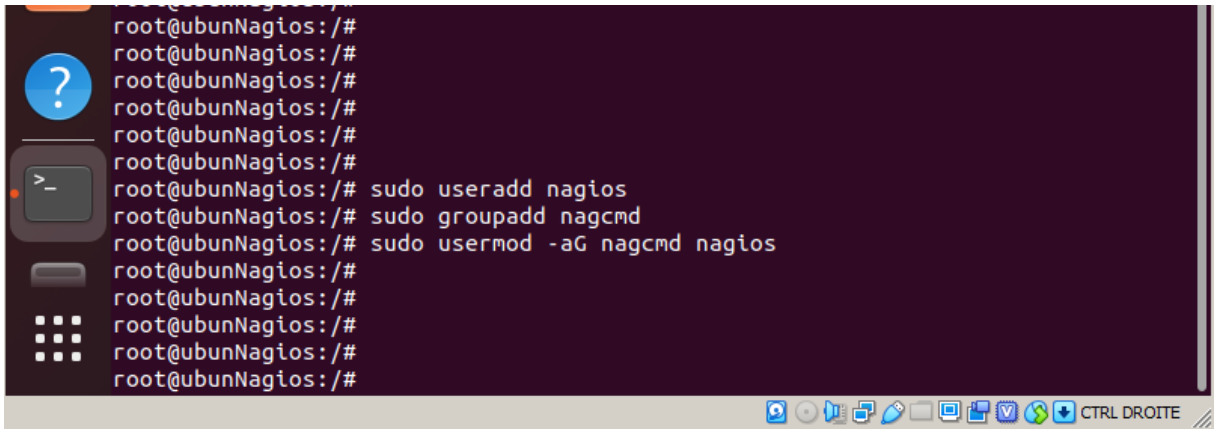
```
sudo apt update && sudo apt upgrade
```

```
sudo apt install wget unzip curl openssl build-essential libgd-dev libssl-dev
libapache2-mod-php php-gdphp apache2 –y
```

```
root@ubunNagios:/# sudo apt update && sudo apt upgrade
Hit:1 http://dz.archive.ubuntu.com/ubuntu kinetic InRelease
Hit:2 http://dz.archive.ubuntu.com/ubuntu kinetic-updates InRelease
Hit:3 http://dz.archive.ubuntu.com/ubuntu kinetic-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu kinetic-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@ubunNagios:/# sudo apt install wget unzip curl openssl build-essential lib
gd-dev libssl-dev libapache2-mod-php php-gd php apache2 -y
```

- ثم إنشاء مستخدم و مجموعته

```
sudo useradd nagios
sudo groupadd nagcmd
sudo usermod –aG nagcmd nagios
```



➢ تثبيت و استخراج Nagios core 4.4.6

wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz

tar -xzf nagios-4.4.6.tar.gz

cd nagios-4.4.6

./configure --with-command-group=nagcmd

sudo make all
sudo make install-groups-users
sudousermod -a -G nagios www-data
sudo make install
sudo make install-daemoninit
sudo make install-commandmode
sudo make install-config
sudo make install-webconf
sudo a2enmod rewrite
sudo a2enmod cgi
sudosystemctl restart apache2

```
sudo make all
sudo make install-groups-users
sudo usermod -a -G nagios www-data
sudo make install
sudo make install-daemoninit
sudo make install-commandmode
sudo make install-config
sudo make install-webconf
sudo a2enmod rewrite
sudo a2enmod cgi
sudo systemctl restart apache2
```

- تثبيت و استخراج ملحقات ناجيوس (Nagios-Plugins) :

wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
tar -xzf nagios-plugins-2.3.3.tar.gz
cd nagios-plugins-2.3.3
./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl

```
root@ubunNagios:/#
root@ubunNagios:/# wget https://nagios-plugins.org/download/nagios-plugins-2.3.
3.tar.gz
--2023-05-01 23:19:30--  https://nagios-plugins.org/download/nagios-plugins-2.3
.3.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org)... 45.56.123.251
Connecting to nagios-plugins.org (nagios-plugins.org)|45.56.123.251|:443... con
nected.
HTTP request sent, awaiting response... 200 OK
Length: 2782610 (2.7M) [application/x-gzip]
Saving to: ‘nagios-plugins-2.3.3.tar.gz’

nagios-plugins-2.3. 100%[==================>]   2.65M  1.23MB/s    in 2.2s

2023-05-01 23:19:33 (1.23 MB/s) - ‘nagios-plugins-2.3.3.tar.gz’ saved [2782610/
2782610]

root@ubunNagios:/#
root@ubunNagios:/# tar -xzf nagios-plugins-2.3.3.tar.gz
root@ubunNagios:/# cd nagios-plugins-2.3.3
root@ubunNagios:/nagios-plugins-2.3.3# ./configure --with-nagios-user=nagios --
with-nagios-group=nagios --with-openssl
```

make
sudo make install

- ضبط اسم المستخدم و كلمة السر

sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

```
root@ubunNagios:/#
root@ubunNagios:/#
root@ubunNagios:/# sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagios
admin
New password:
Re-type new password:
Adding password for user nagiosadmin
root@ubunNagios:/#
```

- التحقق من وجود اخطاء

sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

```
Running pre-flight check on configuration data...

Checking objects...
        Checked 19 services.
        Checked 2 hosts.
        Checked 1 host groups.
        Checked 0 service groups.
        Checked 1 contacts.
        Checked 1 contact groups.
        Checked 26 commands.
        Checked 5 time periods.
        Checked 0 host escalations.
        Checked 0 service escalations.
Checking for circular paths...
        Checked 2 hosts
        Checked 0 service dependencies
        Checked 0 host dependencies
        Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight chec
k
```

- بدا تشغيل Nagios et apache2

sudo systemctl restart apache2

sudo systemctl enable apache2

sudo systemctl restart nagios

sudo systemctl enable nagios

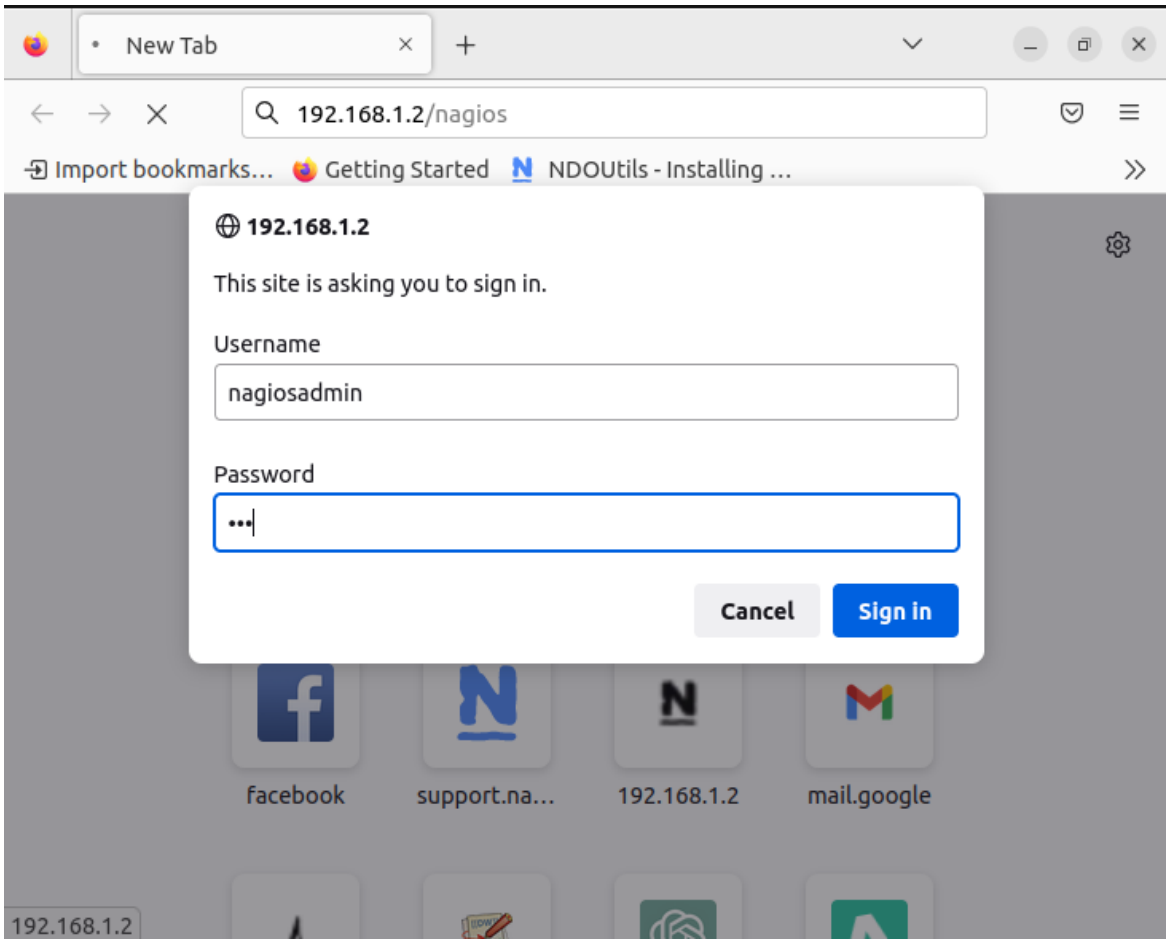
```
sudo systemctl start apache2
sudo systemctl start nagios
sudo systemctl enable nagios
sudo systemctl enable apache2
```

- في متصفح ويب

http://nagios_server_public_ip/nagios

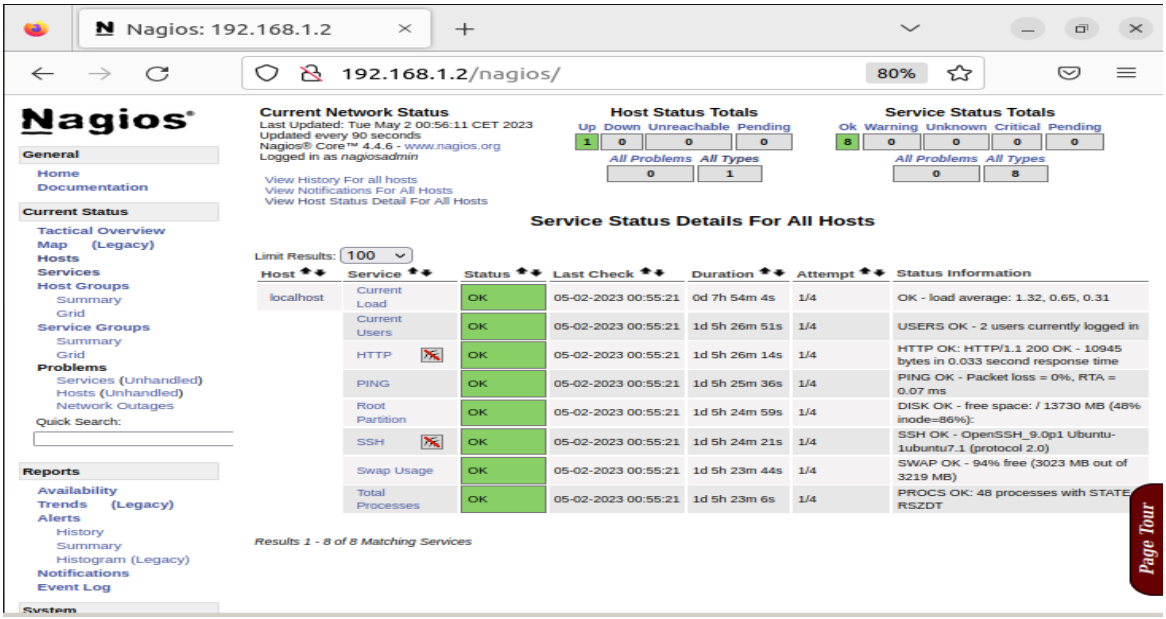
http://192.168.1.2/nagios

- ادخل اسم المستخدم و كلمة السر



الشكل رقم 33 واجهة إدخال اسم المستخدم وكلمة السر

➢ واجهة ناجيوس بعد استكمال التثبيت



الشكل رقم 34 واجهة ناجيوس بعد استكمال التثبيت

4- 1 تعديل المنافذ

يتم تعديل منافذ خاصة في ناجيوس مثل منافذ Apache وssh للسماح بتنفيذ المراقبة اللازمة على الأجهزة وجمع البيانات اللازمة لتحليل أداء النظام وتوفير الإشعارات المطلوبة.

ويمكن تعديل هذه المنافذ في ناجيوس بسهولة من خلال التعديل على ملفات التكوين الخاصة بالنظام

لتعديل القيم المطلوبة لمنافذ Apache و ssh لذلك لدينا بعض الأوامر :

```
for svc in Apache ssh
> do
>ufw allow $svc
> done
ufw enable
```

```
root@ubunNagios:/nagios-4.4.6#
root@ubunNagios:/nagios-4.4.6# for svc in Apache ssh
> do
> ufw allow $svc
> done
Skipping adding existing rule
Skipping adding existing rule (v6)
Skipping adding existing rule
Skipping adding existing rule (v6)
root@ubunNagios:/nagios-4.4.6#
```

✓ وهذه بعض المنافذ الأخرى اللازمة لضمان السير الحسن لNRPE والإشعارات و http :

```
sudo ufw allow 5666/tcp
sudo ufw allow 80/tcp
sudo ufw allow smtp
sudo ufw allow 443/tcp
sudo systemctl restart ufw
```

```
root@ubunNagios:/nagios-4.4.6# ufw status  numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 5666/tcp                   ALLOW IN    Anywhere
[ 2] 80/tcp                     ALLOW IN    Anywhere
[ 3] 443/tcp                    ALLOW IN    Anywhere
[ 4] 25/tcp                     ALLOW IN    Anywhere
[ 5] Apache                     ALLOW IN    Anywhere
[ 6] 22/tcp                     ALLOW IN    Anywhere
[ 7] 5666/tcp (v6)              ALLOW IN    Anywhere (v6)
[ 8] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 9] 443/tcp (v6)               ALLOW IN    Anywhere (v6)
[10] 25/tcp (v6)                ALLOW IN    Anywhere (v6)
[11] Apache (v6)                ALLOW IN    Anywhere (v6)
[12] 22/tcp (v6)                ALLOW IN    Anywhere (v6)

root@ubunNagios:/nagios-4.4.6#
```

4- 2 أداة تحليل البيانات Nagios graph

Nagios graphهي إضافة مجانية لنظام مراقبة الشبكات ناجيوس المفتوح المصدر. تساعد Nagios graphعلى إنشاء رسوم بيانية وتقارير تفصيلية لمراقبة أداء النظام والشبكة بطريقة أكثر سهولة وتفصيلاً. وتستند Nagios graph إلى RRDtool ، وهو أداة مفتوحة المصدر لإنشاء مخططات الرسوم البيانية.

باستخدام Nagios graph ، يمكن للمستخدمين الحصول على نظرة شاملة على أداء النظام على مدار فترات زمنية محددة ، وتحديد الأحداث التي أثرت على أداء النظام ، وتحليل البيانات المرئية لتحديد مشكلات الأداء وتحديد الاتجاهات الاستهلاكية.

يعتبر Nagios graph أداة مفيدة للمسؤولين الذين يرغبون في مراقبة أداء شبكاتهم ونظمهم بطريقة مبسطة وسهلة الاستخدام وبصورة مرئية.

يمكن تثبيته بالخطوات التالية :

- تثبيت وتحميل المتطلبات الأساسية

```
apt-get install libcgi-pm-perllibrrds-perl libgd-gd2-perl
```

- تحميل و استخراج nagios-graph

```
cd ~
wget
http://downloads.sourceforge.net/project/nagiosgraph/nagiosgraph/1.5.2/nag
iosgraph-1.5.2.tar.gz
tar -xzf nagiosgraph-1.5.2.tar.gz
./install.pl --check-prereq
```

```
root@ubunNagios:~# tar -xzf nagiosgraph-1.5.2.tar.gz
root@ubunNagios:~# cd nagiosgraph-1.5.2
root@ubunNagios:~/nagiosgraph-1.5.2#  ./install.pl --check-prereq
checking required PERL modules
  Carp...1.52
  CGI...4.54
  Data::Dumper...2.179
  Digest::MD5...2.58
  File::Basename...2.85
  File::Find...1.39
  MIME::Base64...3.16
  POSIX...1.97
  RRDs...1.7002
  Time::HiRes...1.9767
checking optional PERL modules
  GD...2.76
  Nagios::Config... ***FAIL***
checking nagios installation
  found nagios exectuable at /usr/local/nagios/bin/nagios
checking web server installation
  found apache executable at /usr/sbin/apache2
  found apache init script at /etc/init.d/apache2
root@ubunNagios:~/nagiosgraph-1.5.2#
```

- استخراج الملفات ، و الانتقال إلى دليل التثبيت وتشغيل ملف البرنامج الموجود فيه

```
./install.pl --layout standalone --prefix /usr/local/nagiosgraph
```

```
username or userid of web server user? [www-data]
Modify the Nagios configuration? [n] y
Path of Nagios configuration file? [/usr/local/nagios/etc/nagios.cfg]
Path of Nagios commands file? [/usr/local/nagios/etc/objects/commands.cfg]
Modify the Apache configuration? [n] y
Path of Apache configuration directory?
```

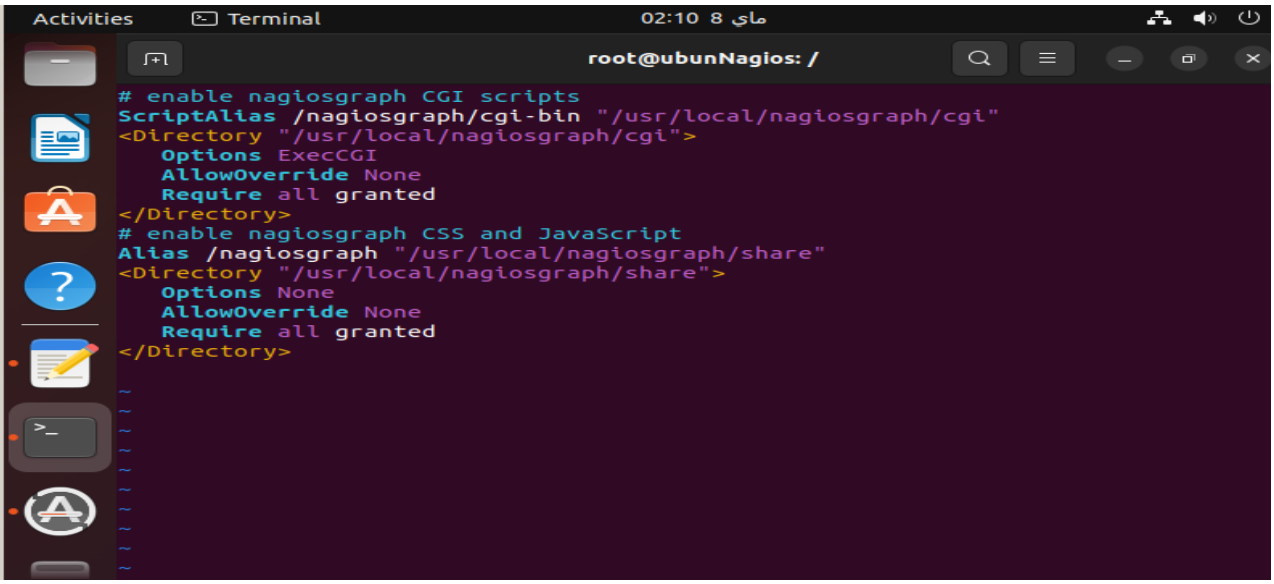
```
  apache_config_dir
  apache_config_file    /etc/apache2/apache2.conf
Continue with this configuration? [y] y
```

- إعادة تشغيل بعض الخدمات

```
service  apache2 restart
service  nagios  restart
```

```
cd  ~
vim  /etc/apache2/sites-enabled/nagiosgraph.conf
```

```
# enable nagiosgraph CGI scripts
 ScriptAlias /nagiosgraph/cgi-bin "/usr/local/nagiosgraph/cgi"
<Directory "/usr/local/nagiosgraph/cgi">
    Options ExecCGI
    AllowOverride None
    Require all granted
</Directory>
# enable nagiosgraph CSS and JavaScript
Alias /nagiosgraph "/usr/local/nagiosgraph/share"
<Directory "/usr/local/nagiosgraph/share">
 Options None
 AllowOverride None
Require all granted
</Directory>
```



- تعديل في Nagios.cfg

```
vim  /usr/local/nagios/etc/nagios.cfg
```

```
# begin nagiosgraph configuration
# process nagios performance data using nagiosgraph
process_performance_data=1
service_perfdata_file=/tmp/perfdata.log
service_perfdata_file_template=$LASTSERVICECHECK$||$HOSTNAME$||$SERVICEDESC$||$
SERVICEOUTPUT$||$SERVICEPERFDATA$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=30
service_perfdata_file_processing_command=process-service-perfdata-for-nagiosgra
ph
# end nagiosgraph configuration
```

- تعديل في commands.cfg

vi /usr/local/nagios/etc/objects/commands.cfg

```
# begin nagiosgraph configuration
# command to process nagios performance data for nagiosgraph
define command {
  command_name process-service-perfdata-for-nagiosgraph
  command_line /usr/local/nagiosgraph/bin/insert.pl
}
# end nagiosgraph configuration
                                                    268,0-1       Bot
```

- تعديل في common-header.ssi :

vim /usr/local/nagios/share/ssi/common-header.ssi

```
<script type="text/javascript" src="/nagiosgraph/nagiosgraph.js"></script>
~
~
```

- تعديل في templates.cfg

vi /usr/local/nagios/etc/objects/templates.cfg

```
#define graph
define service {
      name                graphed-service
      action_url          /nagiosgraph/cgi-bin/show.cgi?host=$HOSTNAME$&service=$
SERVICEDESC$' onMouseOver='showGraphPopup(this)' onMouseOut='hideGraphPopup()'
rel='/nagiosgraph/cgi-bin/showgraph.cgi?host=$HOSTNAME$&service=$SERVICEDESC$&p
eriod=week&rrdopts=-w+450+-j
      register            0
      }
```

- قم بإضافة عبارة graphed-service أمام أي خدمة نريد تمثيلها البياني
- مثلا إذا أردت تعديل ملف localhost

vim /usr/local/nagios/etc/objects/localhost.cfg

```
# Define a service to "ping" the local machine

define service {

    use                     local-service,graphed-service          ; Name of s
ervice template to use
    host_name               localhost
    service_description     PING
    check_command           check_ping!100.0,20%!500.0,60%
}



# Define a service to check the disk space of the root partition
# on the local machine.  Warning if < 20% free, critical if
# < 10% free space on partition.

define service {

    use                     local-service,graphed-service          ; Name of s
ervice template to use
    host_name               localhost
    service_description     Root Partition
    check_command           check_local_disk!20%!10%!/
}
```

- التحقق

sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

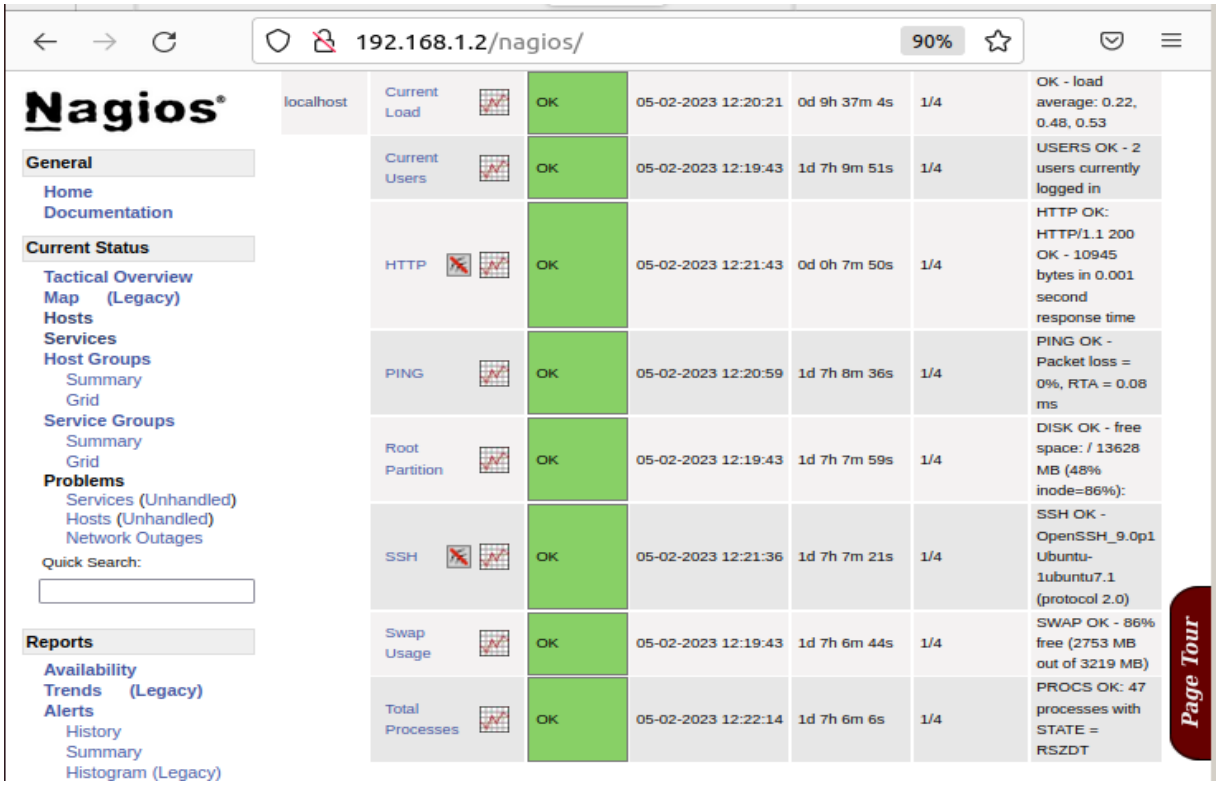
```
Checking objects...
        Checked 8 services.
        Checked 1 hosts.
        Checked 1 host groups.
        Checked 0 service groups.
        Checked 1 contacts.
        Checked 1 contact groups.
        Checked 27 commands.
        Checked 5 time periods.
        Checked 0 host escalations.
        Checked 0 service escalations.
Checking for circular paths...
        Checked 1 hosts
        Checked 0 service dependencies
        Checked 0 host dependencies
        Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight chec
k
root@ubunNagios:~# systemctl restart apache2
root@ubunNagios:~# systemctl restart nagios
root@ubunNagios:~# service nagios restart
root@ubunNagios:~#
```

➢ إعادة تشغيل خدمات apache2 و nagios :

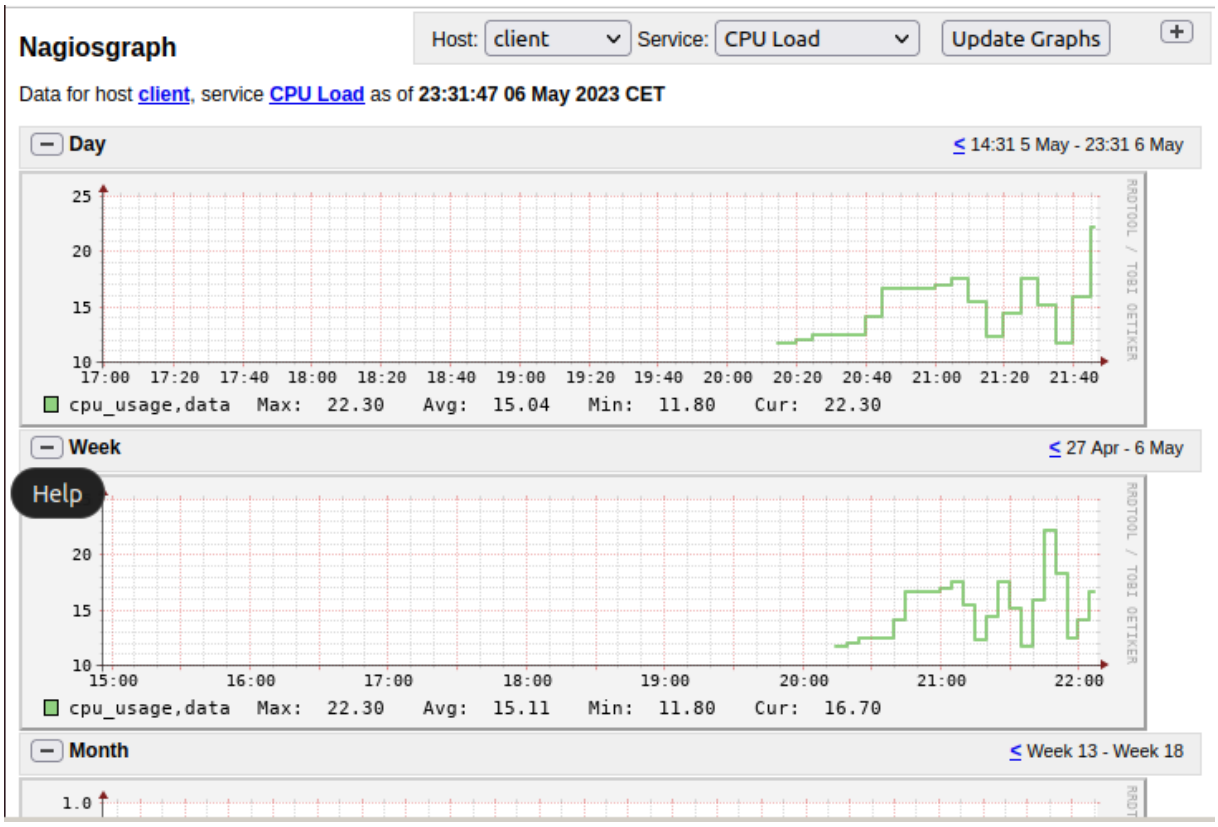
```
systemctl restart apache2
systemctl restart nagios
servicenagios restart
```

➢ شكل واجهة ناجيوس بـNagios graph

```
http://192.168.1.2/nagios/
```



الشكل رقم 35 واجهة الناجيوس الخارجية بعد إضافة الGraph



الشكل رقم 36 عرض ال graph

5-كيفية استخدام أدوات المراقبة المختلفة المتاحة في الناجيوس

توفر الناجيوس العديد من الأدوات المختلفة التي يمكن استخدامها لمراقبة أجهزة الشبكة والخوادم، بما في ذلك NRPE و NS Client++وغيرها. إليكم شرح لكيفية استخدام بعض هذه الأدوات:

NRPE 1-5

يمكن استخدام NRPE (Nagios Remote Plugin Executor) لتحميل البرامج النصية على أجهزة الخوادم المراد مراقبتها وتشغيلها من بعد. يتم تنفيذ هذه البرامج النصية عندما يطلب الناجيوس تشغيلها، ويتم إرسال النتائج إلى الناجيوس للتحليل والعرض. يمكن استخدام NRPE لمراقبة العديد من الأمور مثل القرص الصلب واستخدام الذاكرة والمعالجة وغيرها،لذلك سنقوم بتثبيته داخل ناجيوس أولا ثم على المستخدم الذي نريد مراقبته حسب بعض الأوامر .

5- 1 .1 تثبيته داخل ناجيوس :

- أولا سنقوم بتحديث قائمة الحزم و تثبيت الحزم المطلوبة

```
sudo apt install monitoring-plugins nagios-nrpe-plugin
```

- أنشئ مجلداً جديدًا لتخزين جميع إعدادات مضيفي الخادم الجديد .

```
mkdir  -p /usr/local/nagios/etc/servers
```

- تعديل في ملف nagios.cfg :

```
vim  /usr/local/nagios/etc/nagios.cfg
```

- إضافة سطر

```
cfg_dir=/usr/local/nagios/etc/servers
```

```
# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:
cfg_dir=/usr/local/nagios/etc/servers
#cfg_dir=/usr/local/nagios/etc/servers
#cfg_dir=/usr/local/nagios/etc/printers
#cfg_dir=/usr/local/nagios/etc/switches
#cfg_dir=/usr/local/nagios/etc/routers
```

- قم بتعديل ملفResource.cfg

```
vim  /usr/local/nagios/etc/resource.cfg
```

- قم بإضافة

```
$USER1$=/usr/lib/nagios/plugins
```

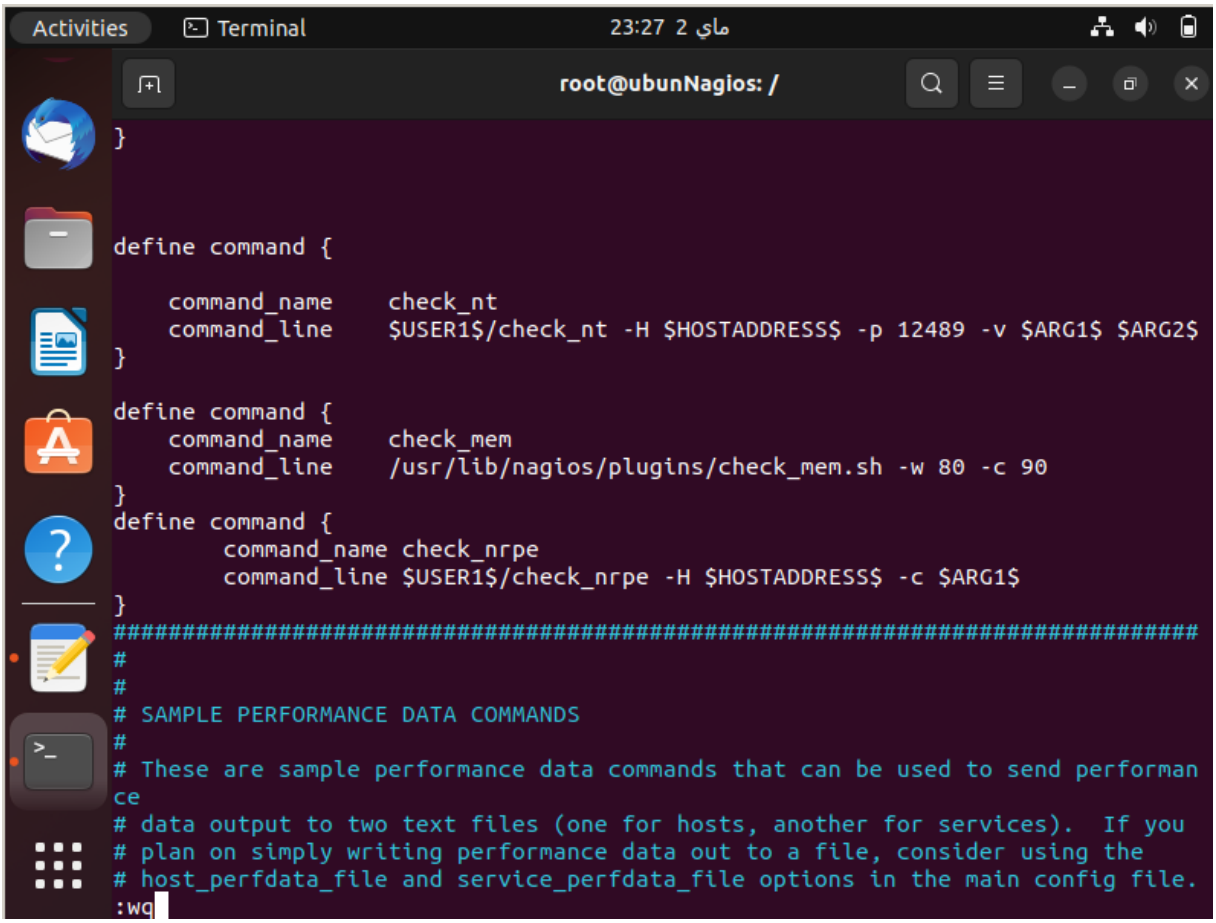
```
# You can define $USERx$ macros in this file, which can in turn be used
# in command definitions in your host config file(s).  $USERx$ macros are
# useful for storing sensitive information such as usernames, passwords,
# etc.  They are also handy for specifying the path to plugins and
# event handlers - if you decide to move the plugins or event handlers to
# a different directory in the future, you can just update one or two
# $USERx$ macros, instead of modifying a lot of command definitions.
#
# The CGIs will not attempt to read the contents of resource files, so
# you can set restrictive permissions (600 or 660) on them.
#
# Nagios supports up to 256 $USERx$ macros ($USER1$ through $USER256$)
#
# Resource files may also be used to store configuration directives for
# external data sources like MySQL...
Text Editor
##############################################################################

# Sets $USER1$ to be the path to the plugins
#$USER1$=/usr/local/nagios/libexec
$USER1$=/usr/lib/nagios/plugins
# Sets $USER2$ to be the path to event handlers
#$USER2$=/usr/local/nagios/libexec/eventhandlers

# Store some usernames and passwords (hidden from the CGIs)
#$USER3$=someuser
#$USER4$=somepassword

                                                              30,1          Bot
```

➢ تعديل الملف object / commands.cfg

```
vim /usr/local/nagios/etc/objects/commands.cfg
```

➢ أضف هذه الأسطر

```
define command {
command_name    check_nrpe
command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
```



الشكل رقم 37 إضافة nrpe للإعدادات

➢ إضافة إعدادات المضيفين (Hosts) إلى خادم ناجيوس

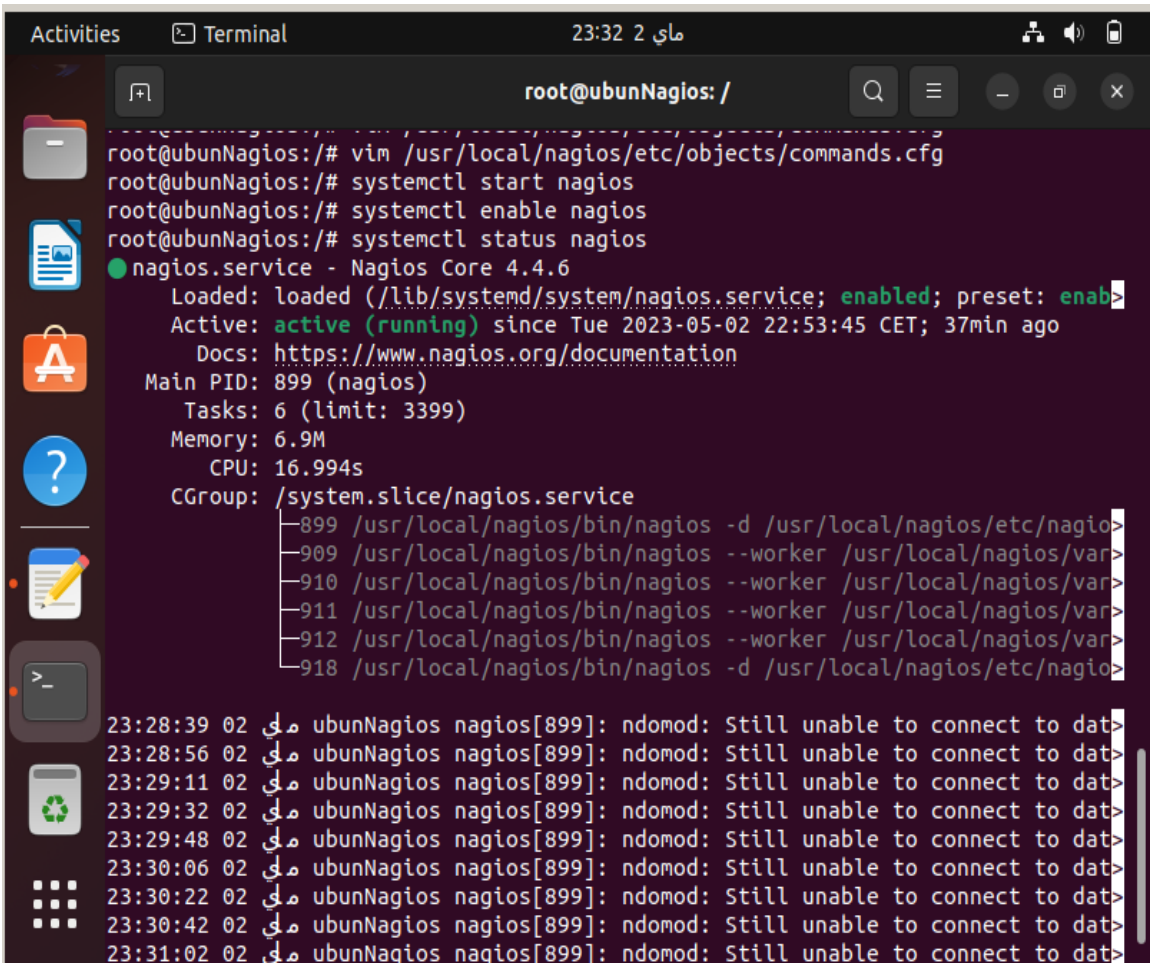
```
vim /usr/local/nagios/etc/servers/client01.cfg
```

```
define host {
      use                 linux-server ; Used template
host_nameclient ; Client name
      alias               Client server ; Description
      address               192.168.1.6 ; IP address ubuntu 2(client01)
max_check_attempts     5
check_period          24x7
notification_interval  30
notification_period    24x7
}
define service {
     use                 generic-service
host_name               client
service_description     PING
check_command           check_ping!100.0,20%!500.0,60%
                                                    }
```

```
define service {
      use                 generic-service,graphed-service
      host_name               client
      service_description     SSH
      check_command           check_ssh                       }
define service {
      use                 generic-service,graphed-service
      host_name               client
      service_description     http
      check_command           check_http                       }
define service{
      use                 generic-service,graphed-service
      host_name               client
      service_description     Memory usage
      check_command           check_nrpe!check_memory       }
define service{
      use                 generic-service,graphed-service
      host_name               client
      service_description     CPU Load
      check_command           check_nrpe!check_cpu           }
define service {
      use                       generic-service,graphed-service
      host_name                 client
      service_description       Current Users
      check_command             check_nrpe!check_users        }
define service{
      use                   generic-service,graphed-service
      host_name               client
      service_description       Swap
      check_command             check_nrpe!check_swap     }
```

➢ التأكد من تشغيل **Nagios**

```
systemctl start nagios
systemctl enable nagios
systemctl status nagios
```



الشكل رقم 38 التأكد من تشغيل Nagios

5-1. 2 تثبيته داخل مستخدم

بعد تثبيت المستخدم الأول (ubuntu) قمنا بإعطائه عنوان IP : 192.168.1.6

➢ قم بتحديث مستودع Ubuntu

```
sudo apt update
sudo apt install nagios-nrpe-server monitoring-plugins
```

- قم بتعديل الملفnrpe.cfg

```
vim /etc/nagios/nrpe.cfg
```

```
server_address= l'addressip of client 1
allowed_hosts=127.0.0.1,::1,L'address de nagios
```

```
server_address=192.168.1.6
```

```
allowed_hosts=127.0.0.1,::1,192.168.1.2
```

- قم بتعديلnrpe_local.cfg

```
vim /etc/nagios/nrpe_local.cfg
```

- قم بإضافة

```
command[check_root]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /
command[check_ping]=/usr/lib/nagios/plugins/check_ping -H 192.168.1.6 -w 100.0,20% -c 500.0,60% -p 5
command[check_ssh]=/usr/lib/nagios/plugins/check_ssh -4 192.168.1.6
command[check_http]=/usr/lib/nagios/plugins/check_http -I 192.168.1.6
command[check_apt]=/usr/lib/nagios/plugins/check_apt
```

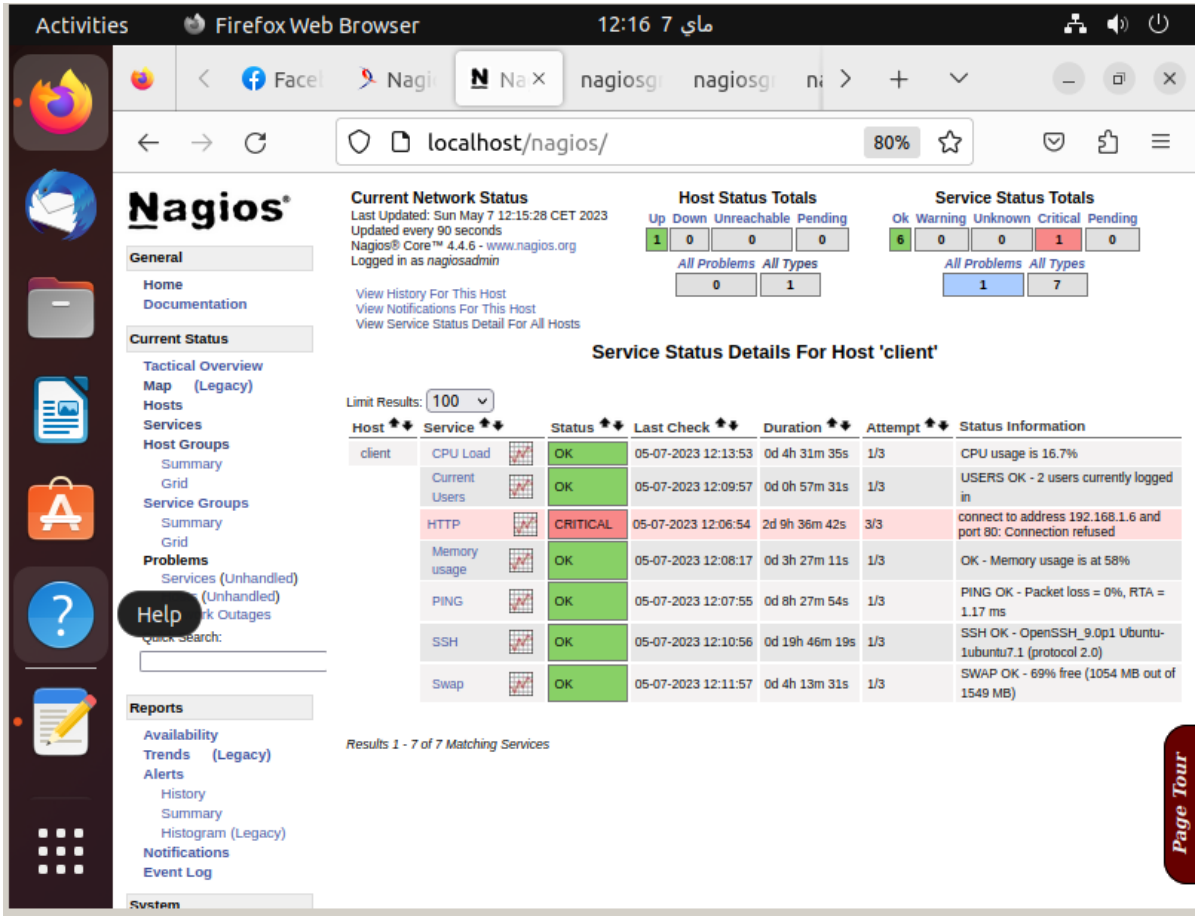
```
##########################################
# Do any local nrpe configuration here
##########################################

 command[check_root]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /
command[check_ping]=/usr/lib/nagios/plugins/check_ping -H 192.168.1.6 -w 100.0,20% -c 500.0,60% -p 5
command[check_ssh]=/usr/lib/nagios/plugins/check_ssh -4 192.168.1.6
command[check_http]=/usr/lib/nagios/plugins/check_http -I 192.168.1.6
command[check_apt]=/usr/lib/nagios/plugins/check_apt
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/nagios/nrpe_local.cfg" 9L, 485B                    6,67          All
```

- التشغيل والتحقق من خدمةNRPE

```
systemctl restart nagios-nrpe-server
systemctl enable nagios-nrpe-server
systemctl status nagios-nrpe-server
```

```
root@client01 ~#
root@client01 ~# cd /etc/nagios
root@client01 /e/nagios#
root@client01 /e/nagios# vim nrpe.cfg
root@client01 /e/nagios#
root@client01 /e/nagios# vim nrpe_local.cfg
root@client01 /e/nagios#
root@client01 /e/nagios# systemctl restart nagios-nrpe-server
root@client01 /e/nagios# systemctl enable nagios-nrpe-server
Synchronizing state of nagios-nrpe-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nagios-nrpe-server
root@client01 /e/nagios#
root@client01 /e/nagios#
```

- واجهة ناجيوس خاصة بالمستخدم client



الشكل رقم 39 واجهة ناجيوس الخاصة بالمستخدم الأول "client"

2-5 NS Client++

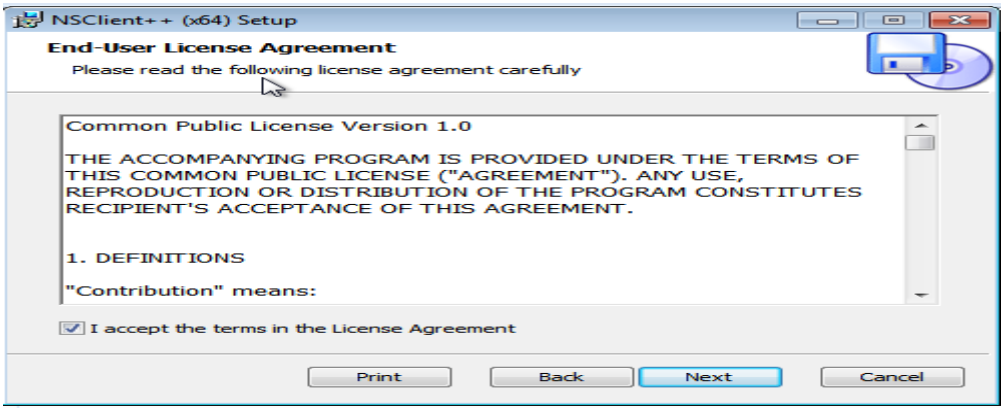
يعد أداة مراقبة مجانية ومفتوحة المصدر يمكن استخدامها للاتصال بأجهزة الخادم ومراقبتها. توفر NS Client++مجموعة متنوعة من الخدمات والوحدات النمطية التي يمكن استخدامها للتحقق من الأمور المختلفة مثل الخدمات والعمليات والشبكات والأقراص وغيرها .

1.2-5 تثبيته داخل المستخدم WINDOWS

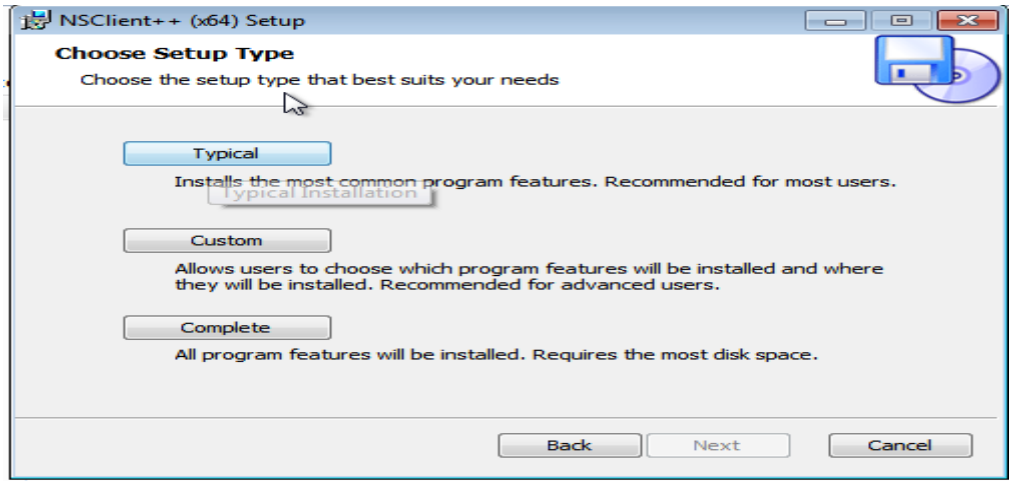
- رابط التحميل :

https ://deac-fra.dl.sourceforge.net/project/nscplus/nscplus/NSClient%2B%2B%200.4.1/NSCP-0.4.1.73-x64.msi

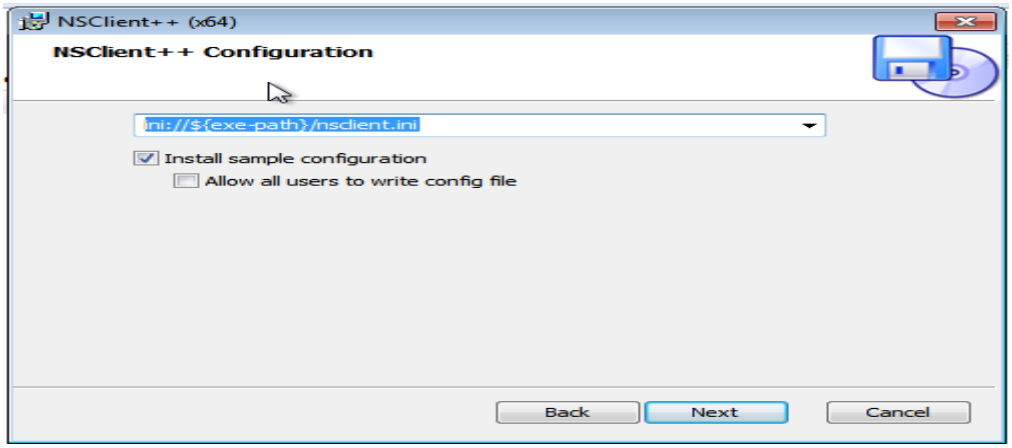
- بعد تحميله نقوم بإتباع الخطوات التالية :



الشكل رقم 40 تأكيد الموافقة الشروط

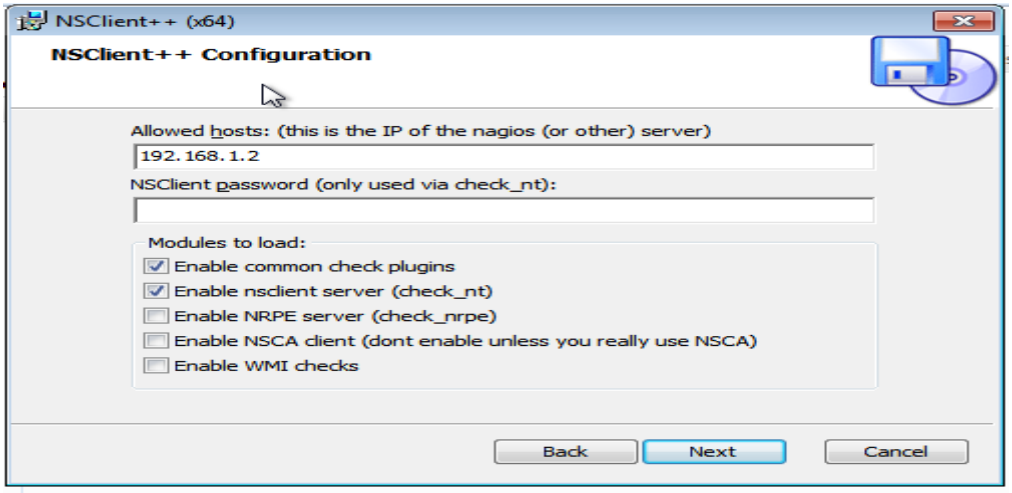


الشكل رقم 41 اختيار النوع



الشكل رقم 42 تثبيت إعدادات NS Client++

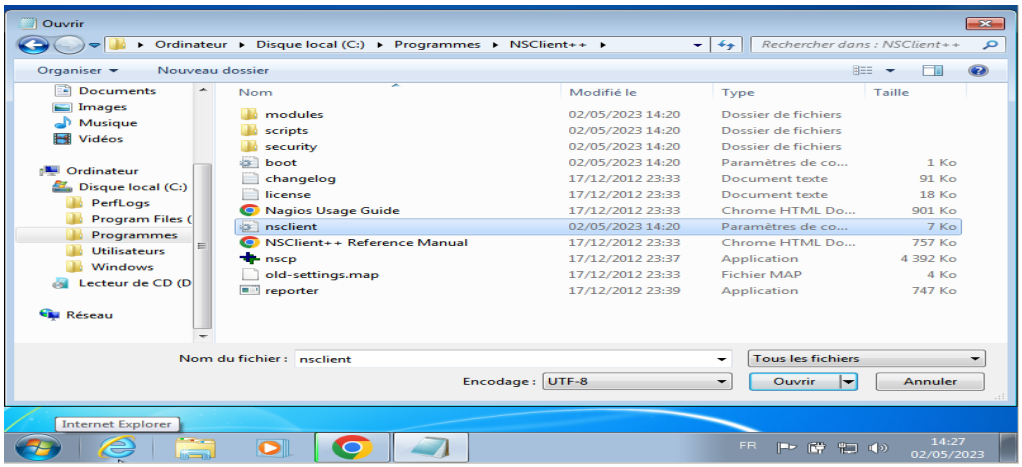
- نضع عنوان IP أو HOSTNAME خادم الناجيوس



الشكل رقم 43 كتابة IP أو HOSTNAME خادم ناجيوس

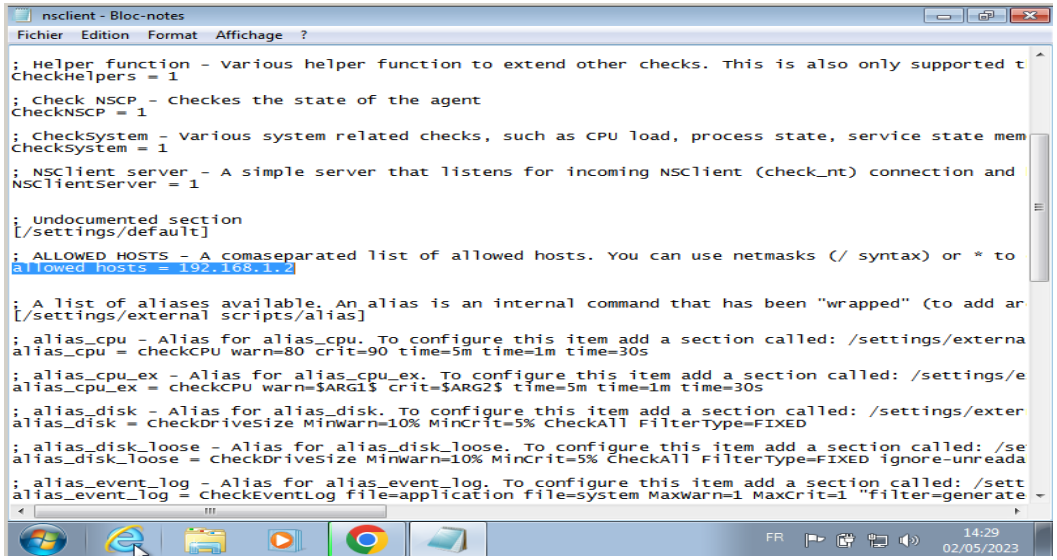
- بعد إتمام الخطوات وتثبيته
- نبحث عن ملف بعنوان NS Client++ غالبا ما يكون في

C:\Program Files\NS Client++



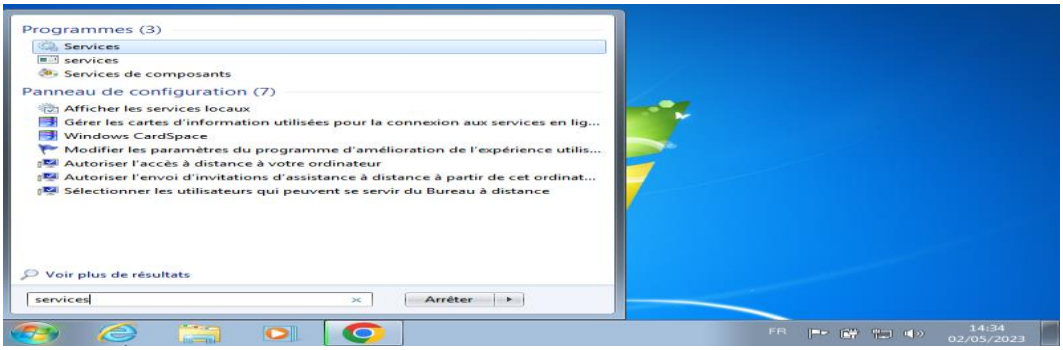
الشكل رقم 44 ننتقل إلى ملف NS Client++

➢ نتأكد من وجود التعليمات التالية :



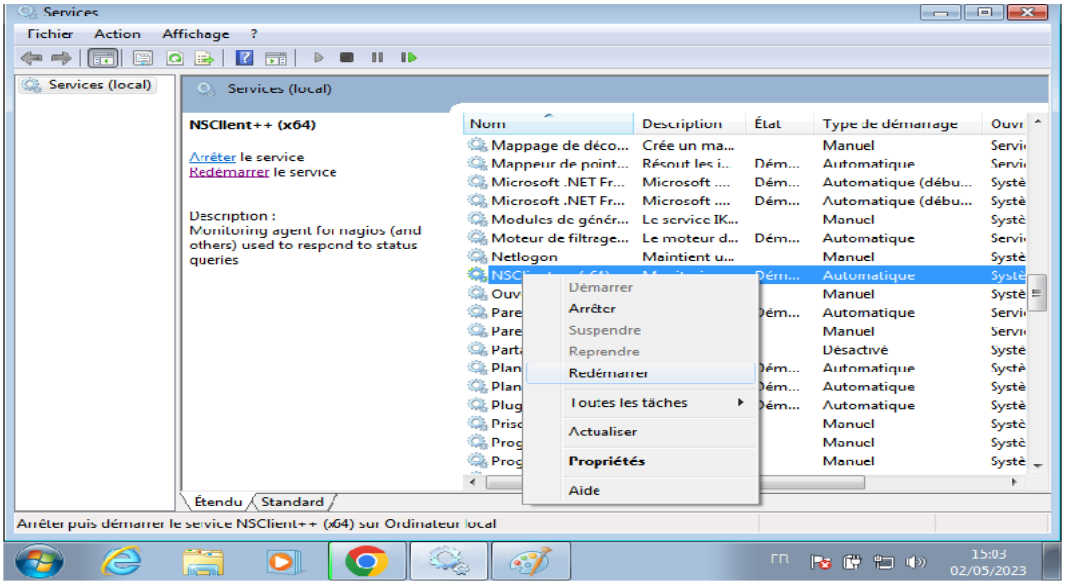
الشكل رقم 45 التحقق من وجود بعض التعليمات الخاصة بـ NS Client++

➢ نبحث عن Services



الشكل رقم 46 ننتقل إلى قائمة services

➢ نقوم بإعادة تشغيل NS CLIENT++



الشكل رقم 47 إعادة تشغيل NS Client++

SNMP 3-5

تستخدم البروتوكولات البسيطة لإدارة الشبكات (SNMP) بشكل شائع للاتصال بأجهزة الشبكة والتحقق من حالتها. تتيح هذه الأداة للمستخدمين جمع المعلومات حول الأجهزة والبرامج المتوفرة على الشبكة، مما يساعد على تحديد المشكلات المحتملة في الوقت الفعلي.

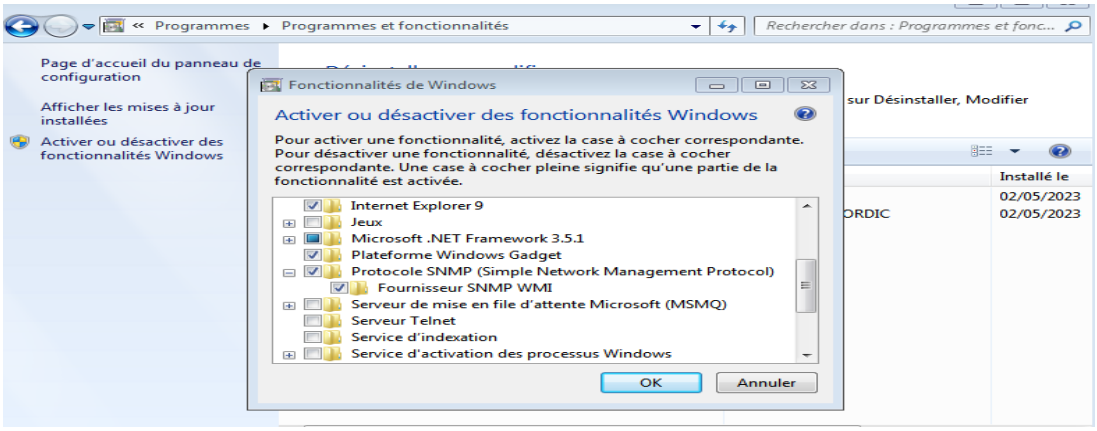
يمكن استخدام هذه الأدوات وغيرها في الناجيوس لتوفير مراقبة شاملة للشبكة و الخوادم وتحليل أدائها.

1.3-5 تعديل SNMP داخل Windows

وهذا تبعا لتعديل بعض الإعدادات الموجودة داخل نظام Windowsالموضحة كالتالي :

✓ **أولا :**

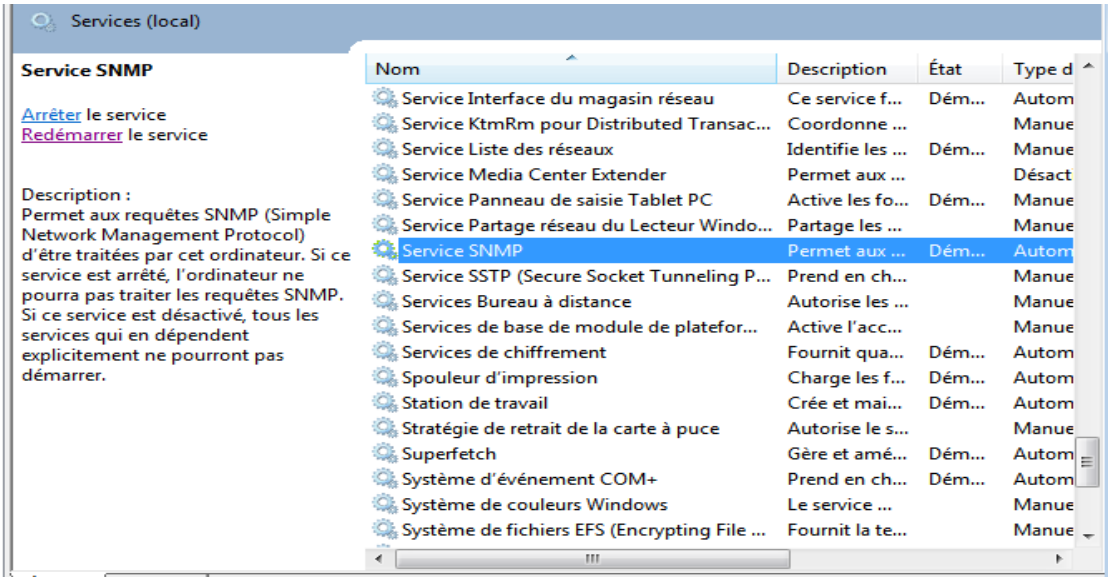
➢ Panneau de configuration\Programmes\Programmes et fonctionnalités
نقوم بشطب SNMP



الشكل رقم 48 تنشيط SNMP

✓ **ثانيا:**

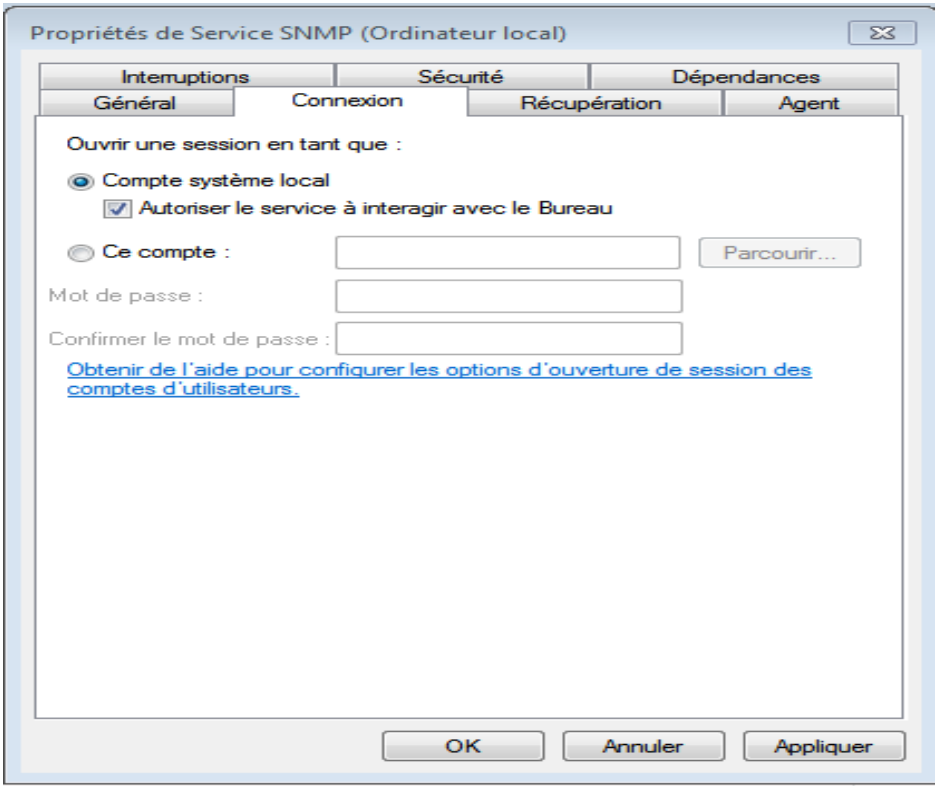
➢ في قائمة service نبحث عن :



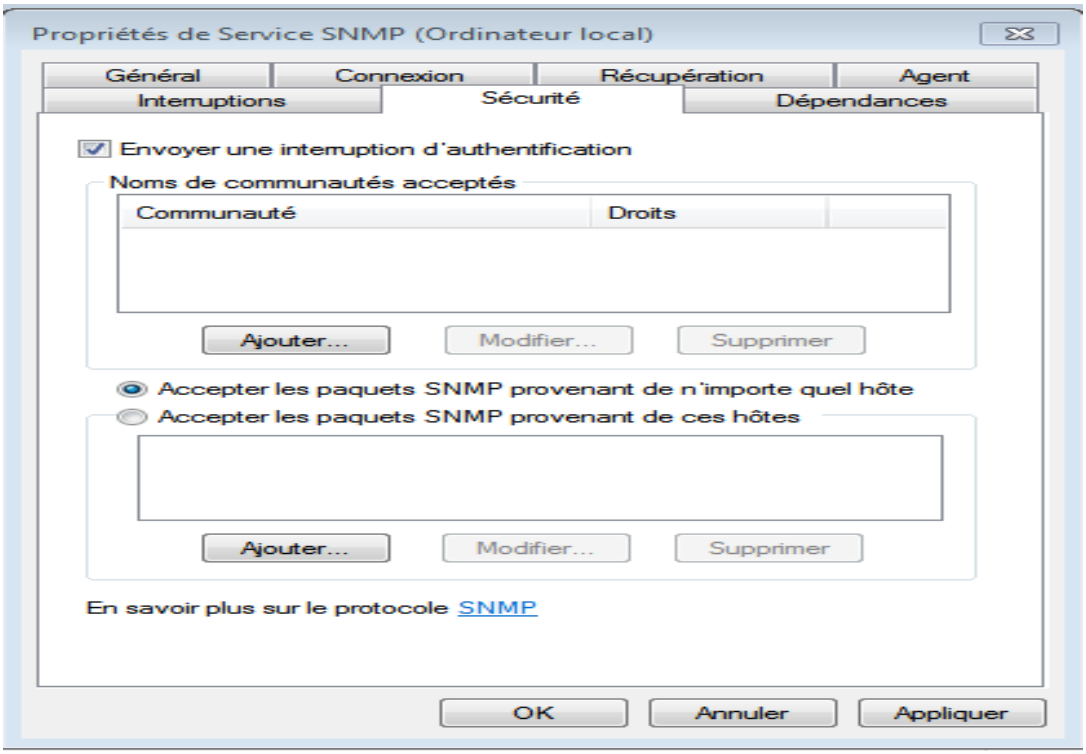
الشكل رقم 49 البحث عن service snmp

✓ **ثالثا :**

➢ نتبع الخطوات التالية :

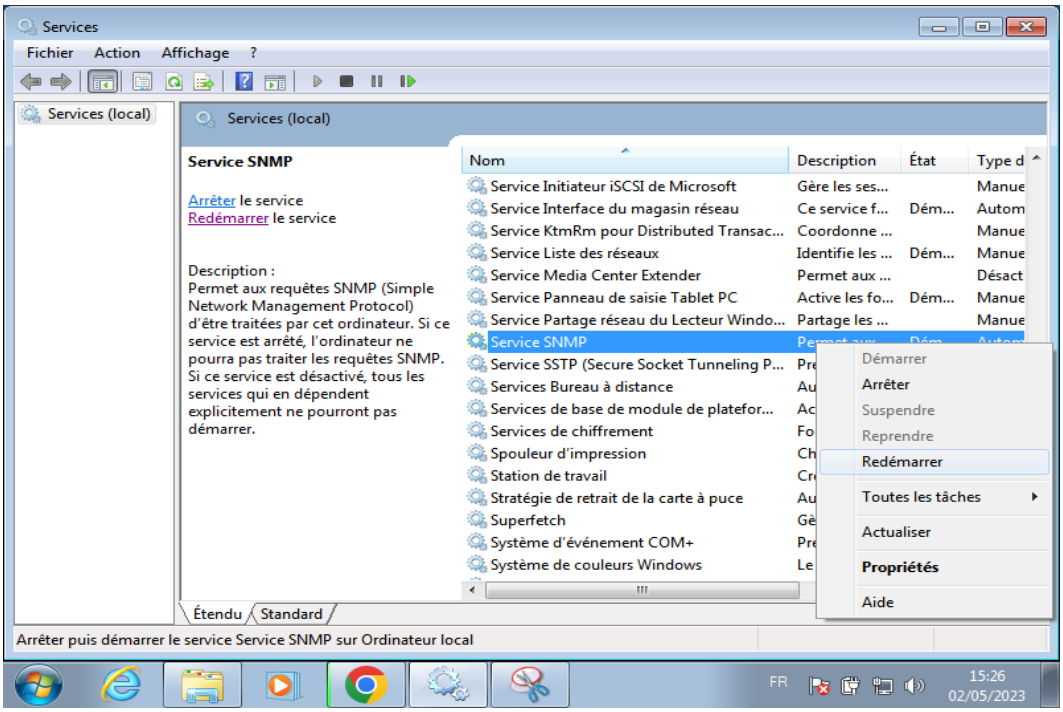


الشكل رقم 50 اعداد الربط



الشكل رقم 51 ضبط حزم SNMP

✓ اعادة تشغيل SNMP:



الشكل رقم 52 اعادة تشغيل SNMP

5-3. 2إضافة windows إلى ناجيوس

- قم بفتح ملف ناجيوس وقم بإضافة المستخدم

```
vim /usr/local/nagios/etc/nagios.cfg
```

- قم بإضافة هذا السطر

```
Cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

```
# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

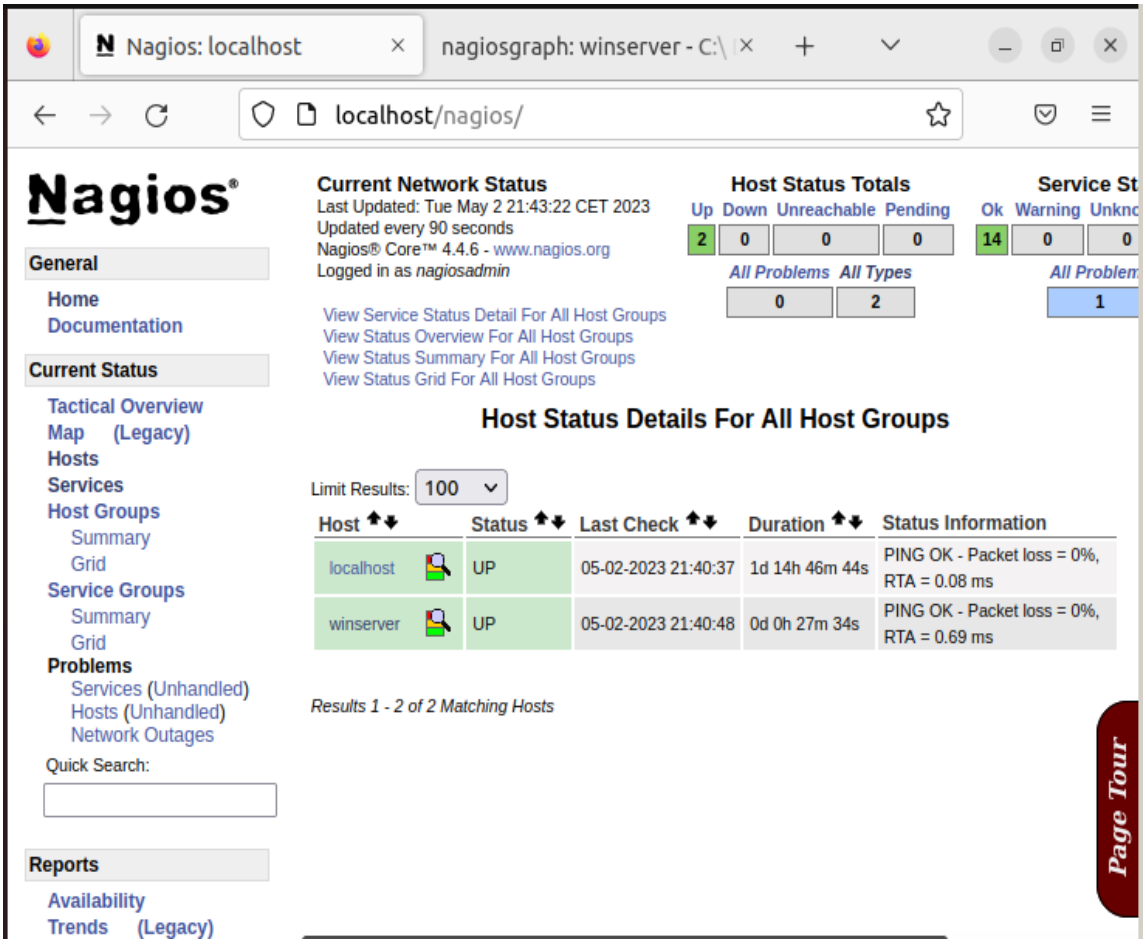
- قم بفتح ملف windows وقم بإضافة الخدمات التي تريد مراقبتها

```
vim /usr/local/nagios/etc/objects/windows.cfg
```

```
# Change the host_name, alias, and address to fit your situation
define host {
   use              windows-server       ; Inherit default values from a template
   host_name          winserver            ; The name we're giving to this host
   alias            My Windows Server      ; A longer name associated with the host
   address            192.168.1.3          ; IP address of the host windows
}
```

```
define service {
   use                generic-service,graphed-service
   host_name          winserver
   service_description    NSClient++ Version
   check_command          check_nt!CLIENTVERSION
}
define service {
   use                generic-service,graphed-service
   host_name          winserver
   service_description    Uptime
   check_command          check_nt!UPTIME
}
define service {
   use                generic-service,graphed-service
   host_name          winserver
   service_description    CPU Load
   check_command          check_nt!CPULOAD!-l 5,80,90
}
define service {
   use                generic-service,graphed-service
   host_name          winserver
   service_description    Memory Usage
   check_command          check_nt!MEMUSE!-w 80 -c 90
}
define service {
   use                generic-service,graphed-service
   host_name          winserver
   service_description    C:\ Drive Space
   check_command          check_nt!USEDDISKSPACE!-l c -w 80 -c 90
}
define service {
   use                generic-service,graphed-service
   host_name          winserver
   service_description    W3SVC
   check_command          check_nt!SERVICESTATE!-d SHOWALL -l W3SVC      }
define service {
   use                generic-service,graphed-service
   host_name          winserver
   service_description    Explorer
   check_command          check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
 }
```

➢ واجهة ناجيوس لمراقبة Windows



الشكل رقم 53 واجهة ناجيوس لمراقبة Windows

6-كيفية إعداد الإشعارات لتلقي تنبيهات عند وجود مشكلات في الشبكة

يمكن لنظام ناجيوس إرسال إشعارات للمسؤولين عن النظام في حالة وجود مشكلات أو خلل في الشبكة. يتم ذلك من خلال تكوين إعدادات و إشعارات في الناجيوس. يمكن تكوين الإشعارات لإرسال رسائل البريد إلكتروني، رسائل نصية SMS أو رسائل عبر تطبيقات التراسل الفوري مثل تيليجرام.

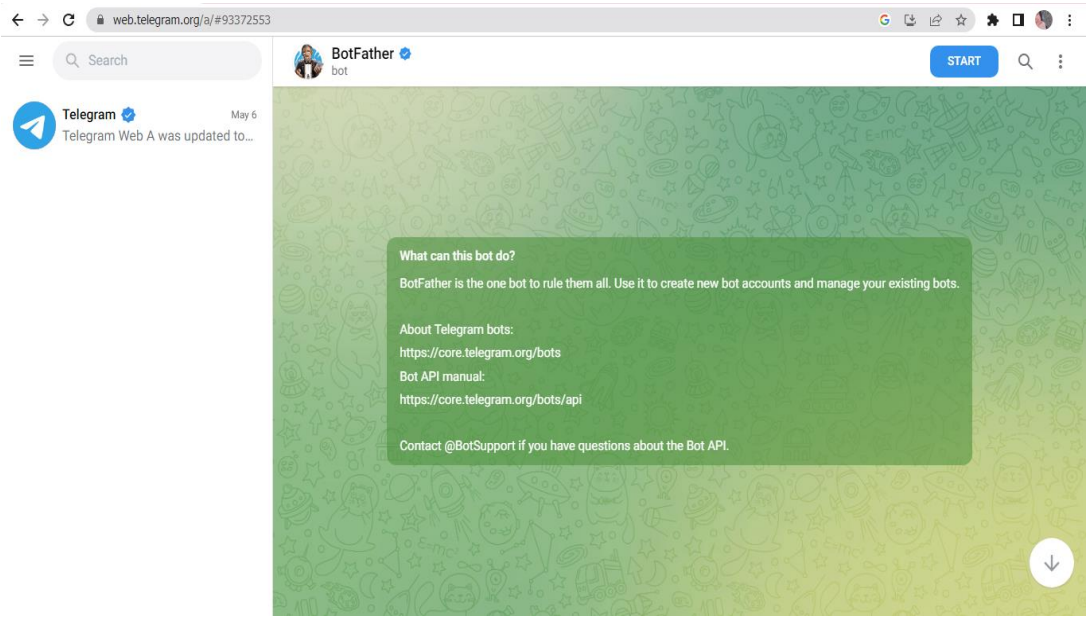
6-1 تعريف تطبيق تيليجرام

تيليجرام هو تطبيق للدردشة والمراسلة الفورية يعمل على الهواتف الذكية والأجهزة اللوحية وأجهزة الكمبيوتر، وهو يستخدم تقنية التشفير لحماية الرسائل والمحادثات المرسلة والمستلمة عبر الإنترنت. يتميز تطبيق تيليجرام بسرعة وسهولة الاستخدام ويتيح إمكانية إرسال الرسائل النصية والصوتية والصور والفيديو والملفات بحجم كبير، كما يوفر إمكانية إنشاء مجموعات وقنوات للتواصل مع الأصدقاء والعائلة والزملاء[10].

6- 2إعداد تنبيهات لإرسال رسائل إلى تطبيق تيليجرام

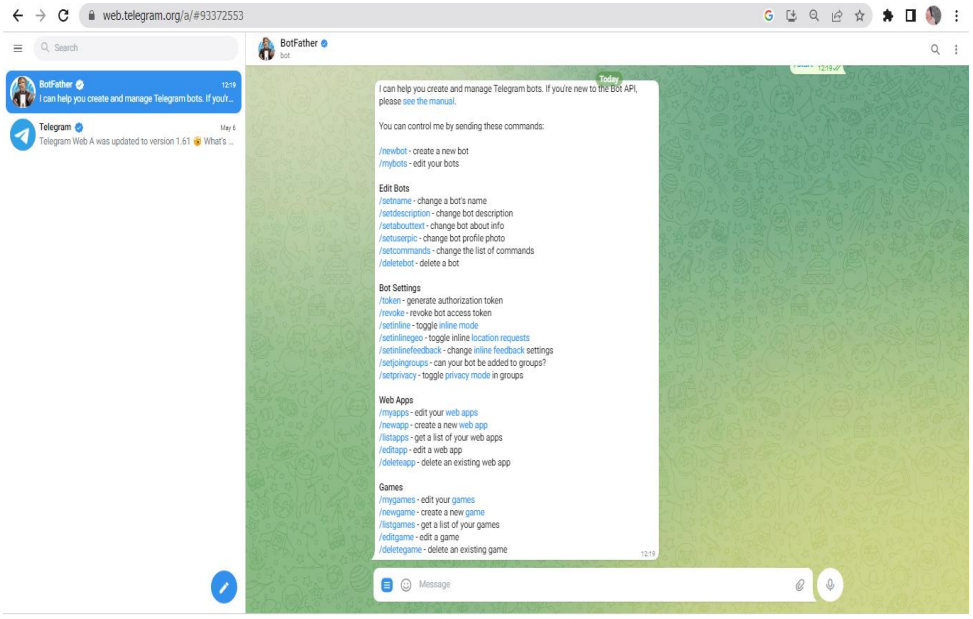
يمكن إعداد تنبيهات لإرسال رسائل إلى تطبيق تيليجرام عند وجود مشكلات في شبكة ناجيوس باستخدام الخطوات التالية:

- ✓ **أولا** قم إنشاء حساب على تطبيق تيليجرام أو على موقع **https://web.telegram.org**
- ✓ **ثانيا** في خانة البحث قم بالبحث عن حساب باسم **BotFather**



الشكل رقم 54 واجهة BotFather

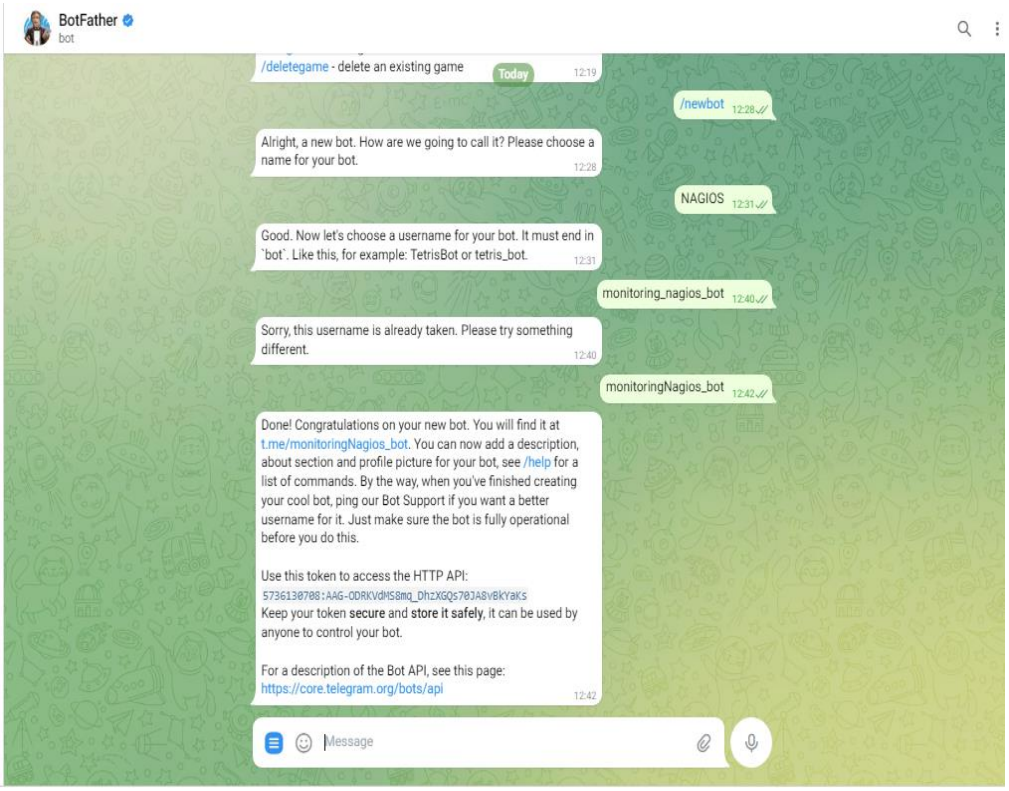
✓ بعد النقر على **START**



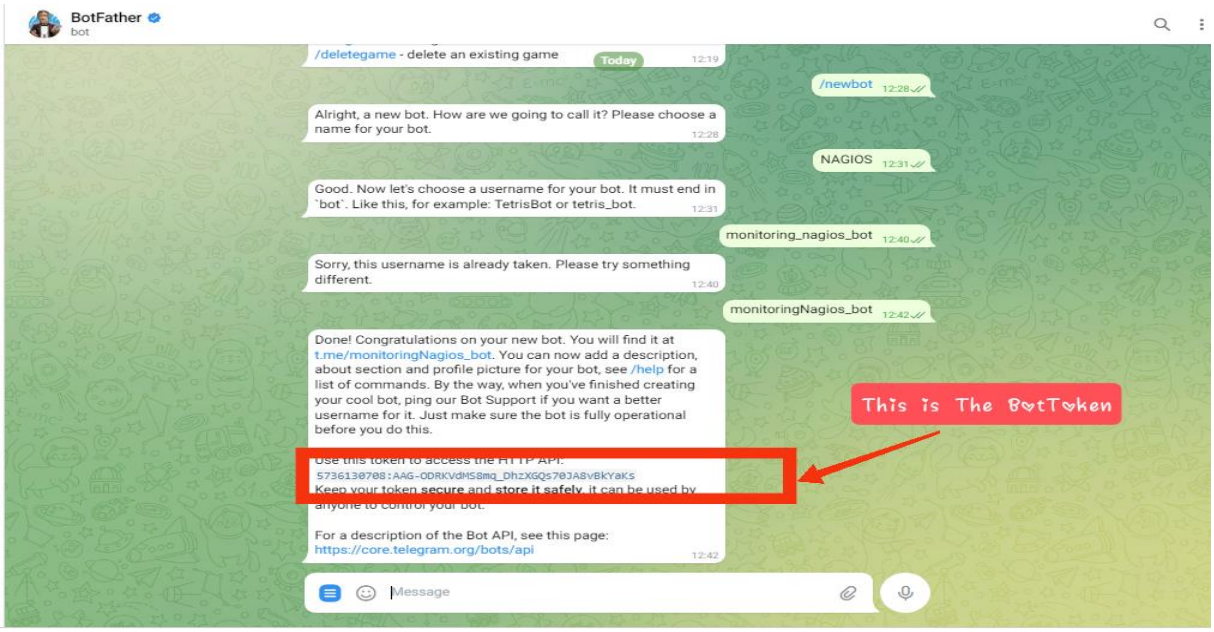
الشكل رقم 55 بداية الاستعمال

✓ نحن بالحاجة إلى إنشاء bot جديد لتلقي الإشعارات
/newbot

✓ نختار اسم البوت واسم المستخدم (**username**)

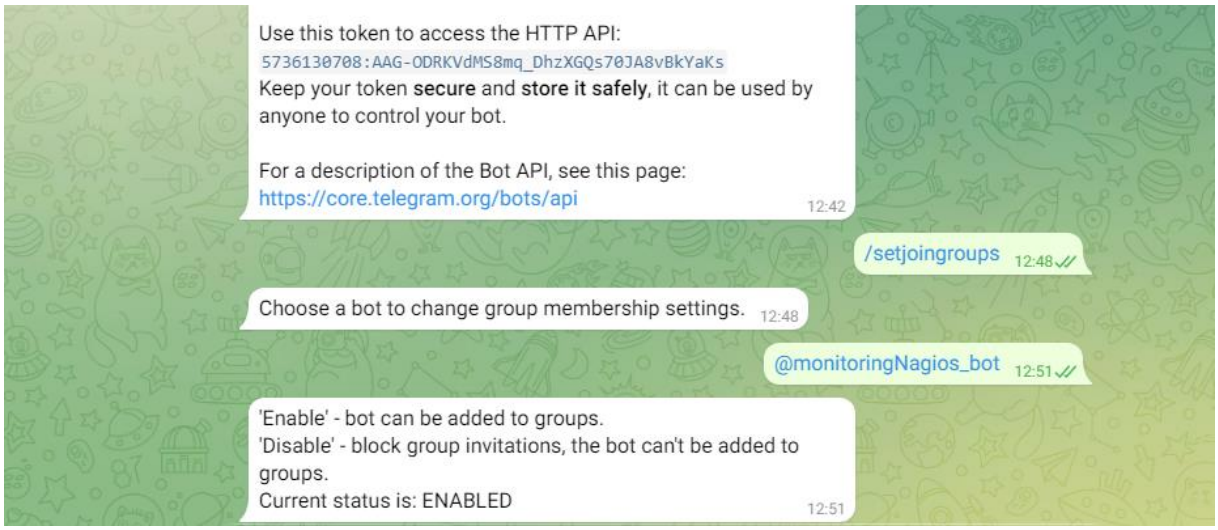


الشكل رقم 56 إنشاء bot جديد و تحديد اسم له



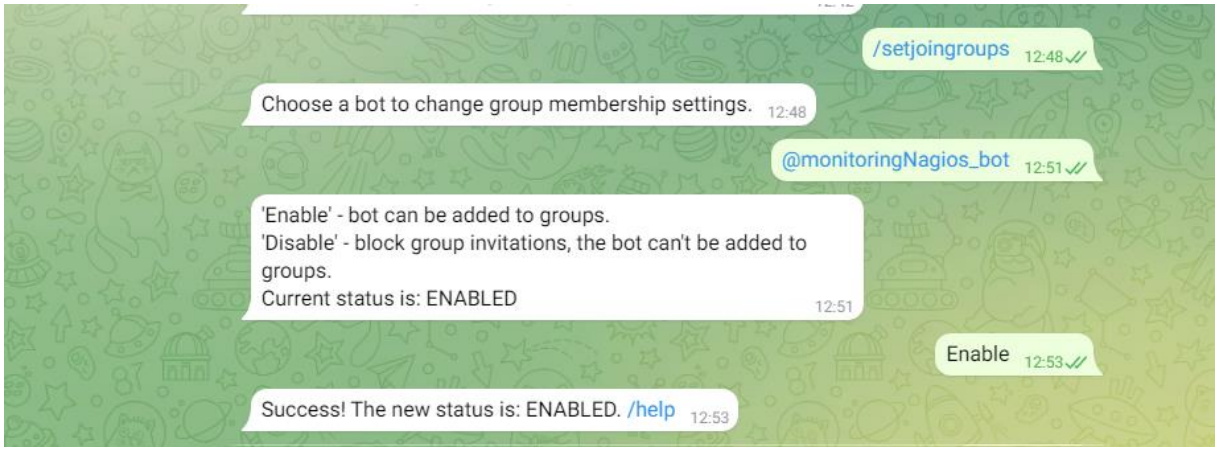
الخاص بنا botToken الشكل رقم 57 رمز ال

✓ بعد إدخال التعليمة التالية **setjoingroups**/ نختار البوت الخاص بنا



الشكل رقم 58 اعدادات اضافية حتى يتمكن البوت من الانضمام تلقائيا للمجموعات الجديدة

✓ نختار **Enable**



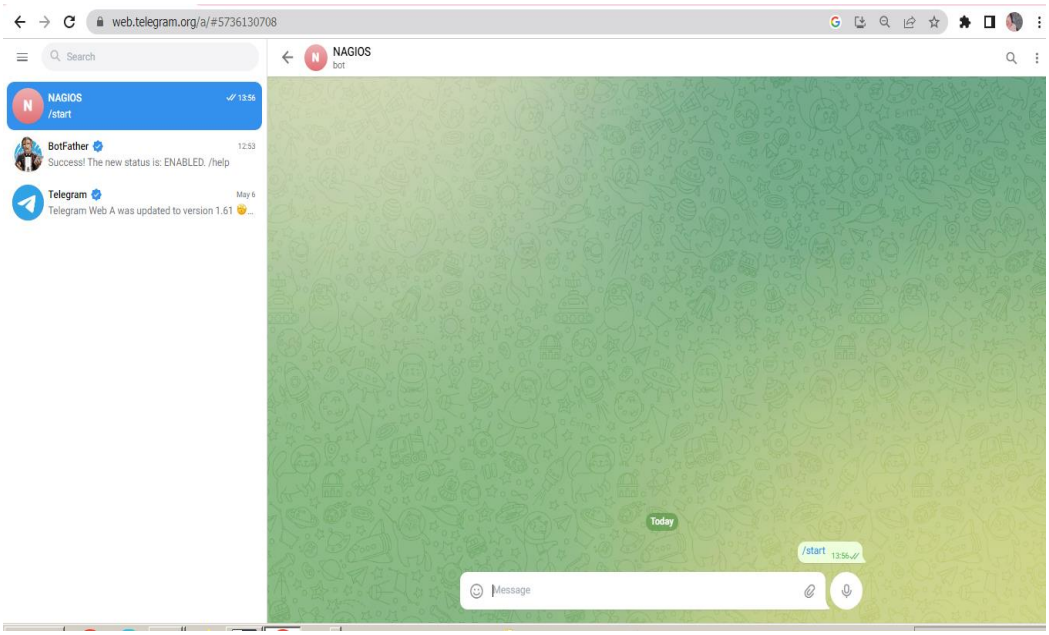
الشكل رقم 59 اختيار Enable

✓ https://api.telegram.org/bot-YourBOTToken-/getUpdates

✓ في البداية ستكون النتيجة كالآتي

الشكل رقم 60 التحقق

✓ نعود ل **botFather** ونقوم بالنقر على اسم مستخدم البوت الذي قمنا بإنشائه ثم زر **START**



الشكل رقم 61 الدخول إلى البوت خاص بنا و تشغيله

✓ نعيد تشغيل الصفحة السابقة يجب أن تكون النتيجة كالآتي حتى نتأكد أن البوت يعمل بشكل صحيح

الشكل رقم 62 التيليجرام ID

✓ الآن ننتقل إلى ناجيوس

✓ بعد فتح **Terminal** ندخل التعليمات التالية :

```
dhclient
curl -POST https://api.telegram.org/bot-YourBOTToken-/getUpdates
```

```
root@ubunNagios:~#
root@ubunNagios:~#
root@ubunNagios:~# dhclient
root@ubunNagios:~# curl -POST https://api.telegram.org/bot5736130708:AAG-ODRKVd
MS8mq_DhzXGQs70JA8vBkYaKs/getUpdates
{"ok":true,"result":[{"update_id":342046879,
"message":{"message_id":1,"from":{"id":5880772829,"is_bot":false,"first_name":"
hayat","last_name":"ilham","language_code":"en"},"chat":{"id":5880772829,"first
_name":"hayat","last_name":"ilham","type":"private"},"date":1684068968,"text":"
/start","entities":[{"offset":0,"length":6,"type":"bot_command"}]}}]}root@ubunN
agios:~#
```

✓ التعديل في ملف **commands.cfg**

Vim /usr/local/nagios/etc/objects/commands.cfg

'notify-host-by-telegram' command definition

define command {

command_name notify-host-by-telegram

command_line /usr/bin/curl -X POST --data chat_id=$CONTACTPAGER$ --data parse_mode="markdown" --data text="%60$HOSTNAME$%60 %0A%0A$NOTIFICATIONTYPE$ %0A%60$HOSTSTATE$%60 %0A%60$HOSTADDRESS$%60 %0A%60$HOSTOUTPUT$%60" https://api.telegram.org/bot-YourBOTToken-/sendMessage

}

'notify-service-by-telegram' command definition

define command {

command_name notify-service-by-telegram

command_line /usr/bin/curl -X POST --data chat_id=$CONTACTPAGER$ --data parse_mode="markdown" --data text="%60$HOSTNAME$%60 %0A%0A$NOTIFICATIONTYPE$ %0A%60$SERVICEDESC$%60 %0A%60$HOSTADDRESS$%60 %0A%60$SERVICESTATE$%60 %0A%60$SERVICEOUTPUT$%60" https://api.telegram.org/bot-YourBOTToken-/sendMessage

```
# 'notify-host-by-telegram' command definition
define command {
        command_name    notify-host-by-telegram
        command_line /usr/bin/curl -X POST --data chat_id=$CONTACTPAGER$ --data par
se_mode="markdown" --data text="%60$HOSTNAME$%60 %0A%0A$NOTIFICATIONTYPE$ %0A%6
0$HOSTSTATE$%60 %0A%60$HOSTADDRESS$%60 %0A%60$HOSTOUTPUT$%60" https://api.teleg
ram.org/bot5736130708:AAG-ODRKVdMS8mq_DhzXGQs70JA8vBkYaKs/sendMessage
  }

# 'notify-service-by-telegram' command definition
 define command {
        command_name    notify-service-by-telegram
        command_line /usr/bin/curl -X POST --data chat_id=$CONTACTPAGER$ --data
 parse_mode="markdown" --data text="%60$HOSTNAME$%60 %0A%0A$NOTIFICATIONTYPE$ %
0A%60$SERVICEDESC$%60 %0A%60$HOSTADDRESS$%60 %0A%60$SERVICESTATE$%60 %0A%60$SER
VICEOUTPUT$%60" https://api.telegram.org/bot5736130708:AAG-ODRKVdMS8mq_DhzXGQs7
0JA8vBkYaKs/sendMessage
}
################################################################################
#
```

LibreOffice Writer

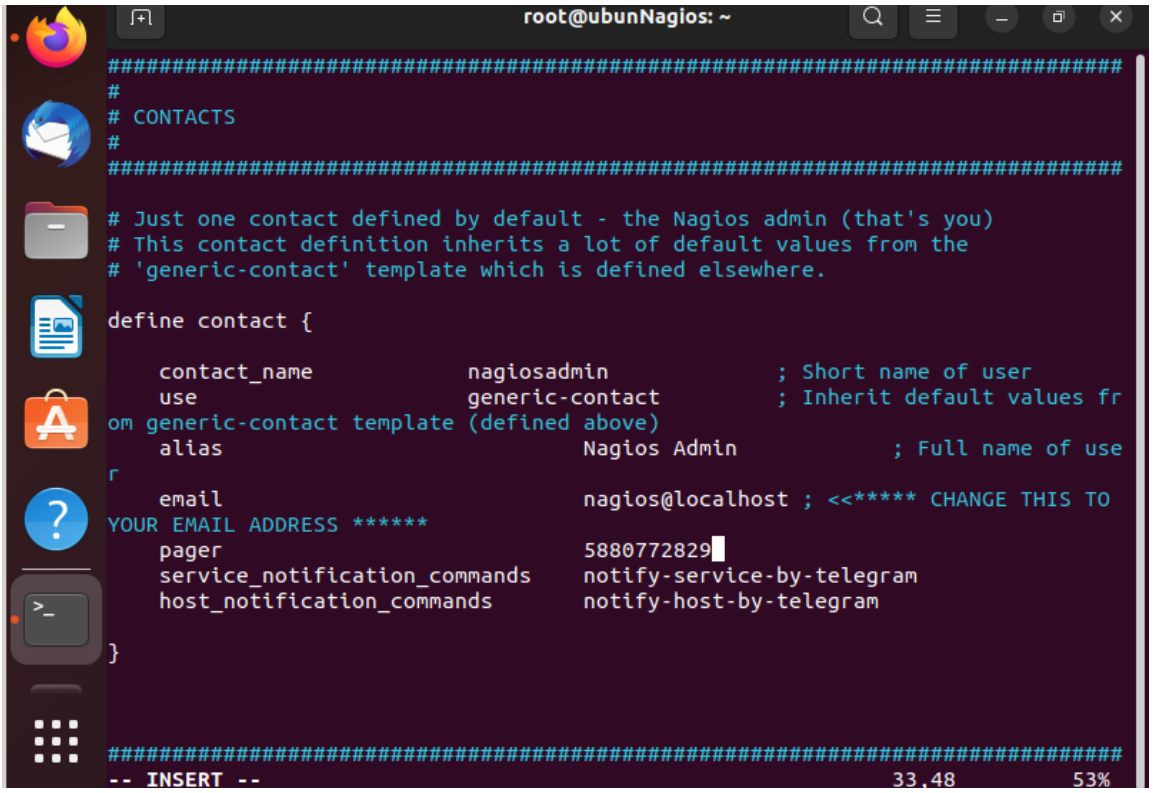
✓ التعديل في ملف **contacts.cfg**

Vim /usr/local/nagios/etc/objects/contacts.cfg

Define contact {

contact_name	nagiosadmin
use	generic-contact
alias	nagios admin ; Full name of user
email	root@localhost
pager	YOUR-TELEGRAM-ID-HERE
service_notification_commands	notify-service-by-telegram
host_notification_commands	notify-host-by-telegram

}



✓ إعادة تشغيل خدمات nagios et apache2

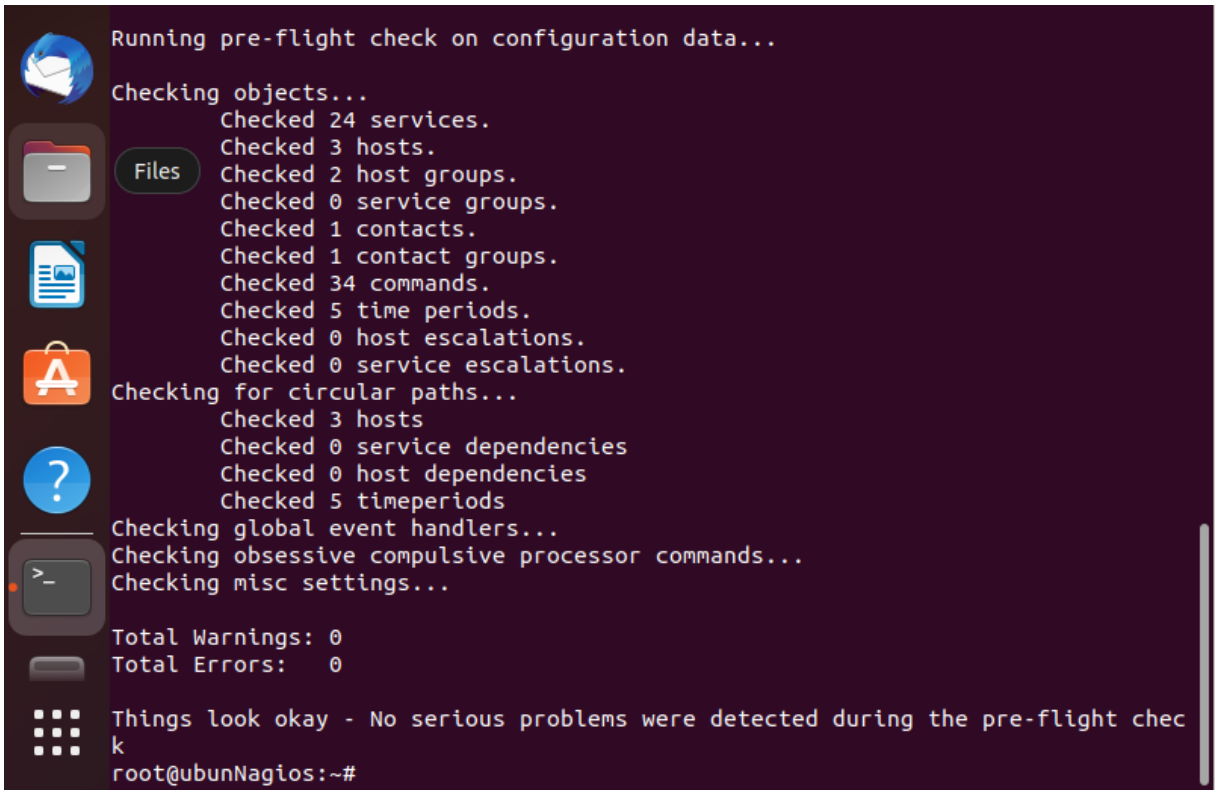
```
Systemctl restart nagios .service apache2.service
```

```
root@ubunNagios:~#
root@ubunNagios:~#
root@ubunNagios:~# systemctl restart nagios.service  apache2.service
```

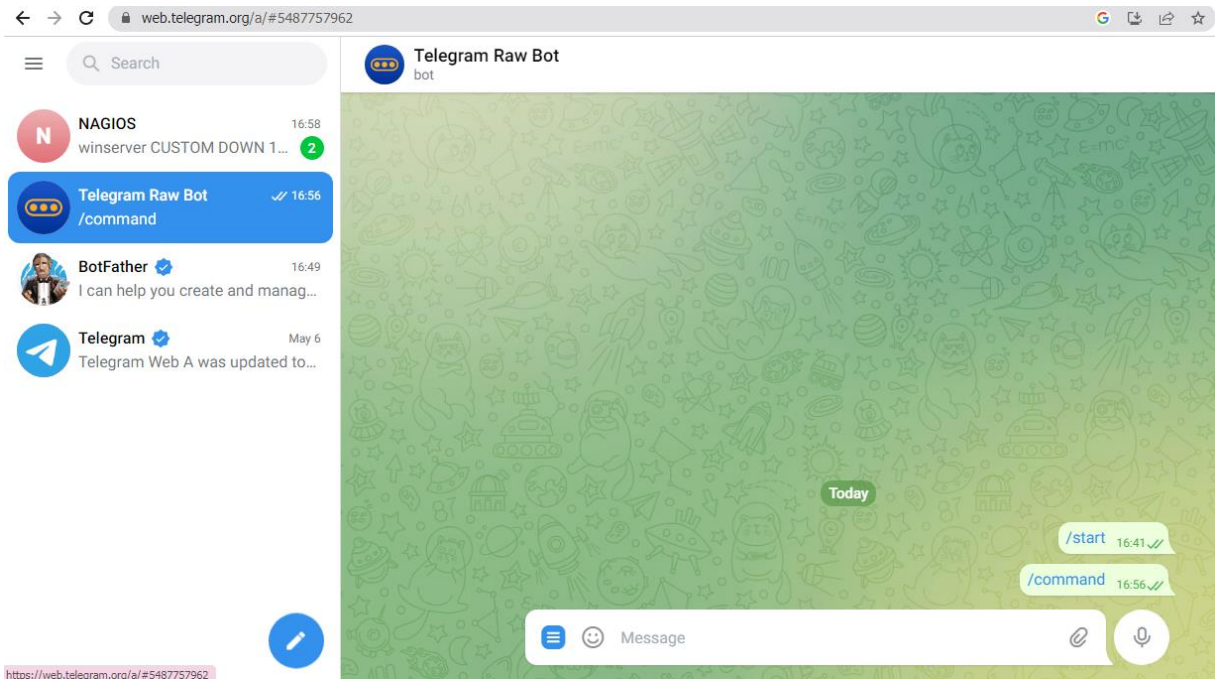
✓ التحقق من وجود أخطاء

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

✓ بالطريقة المعتادة نقوم بالدخول لواجهة ناجيوس

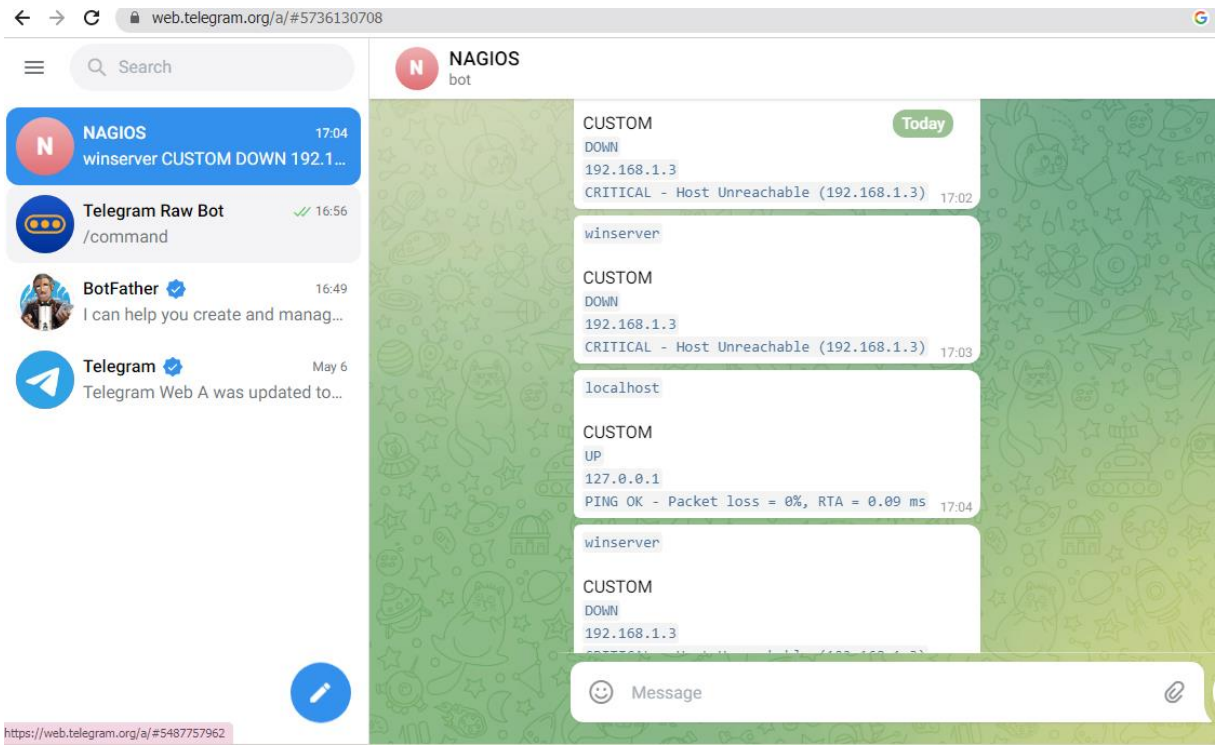


✓ نعود للتيليجرام ونبحث عن بوت أخر باسم Telegram Raw bot ونضغط START لبدء تشغيله



الشكل رقم 63 بحث عن Telegram Raw bot وتشغيله

✓ الآن ستلاحظ بدء استلام الإشعارات الخاصة بناجيوس في البوت الخاص بك



الشكل رقم 64 بدء استلام الاشعارات في البوت

خاتمة

بهذا نكون قد انتهينا من فصل تطبيق شبكة ناجيوس، حيث قمنا بتقديم نظرة شاملة على كيفية استخدامها لمراقبة الخوادم والأنظمة والتطبيقات. كما تم توضيح الأدوات المستخدمة للمراقبة والإشعار والتنبيه عند حدوث أي مشكلة في النظام. وقد تم شرح بعض الأمثلة العملية وكيفية تحليل البيانات المتاحة لتحسين أداء النظام وتفادي المشكلات المحتملة في المستقبل.

ومن المؤكد أن استخدام شبكة ناجيوس قد يحتاج إلى بعض الخبرة والمعرفة في الإعداد والتكوين، لكنها تعتبر أداة قوية وفعالة لمراقبة النظام والتأكد من استمرارية الخدمات والتطبيقات. لذلك، ننصح بإدخالها ضمن خطط الصيانة والإدارة الاستباقية للنظام وتحسين أداءه.

خاتمة عامة

باختصار، تمت دراسة Nagios كأداة مراقبة وإدارة الشبكات ونظام المراقبة المستمرة للخدمات والأنظمة. وتم توضيح أهمية استخدام أدوات المراقبة والإنذار للحفاظ على أداء الشبكة وتقليل الأعطال وتوفير الوقت والجهد في إصلاح المشكلات. وتم تقديم نظرة عامة على مكونات Nagios وطريقة عمله، بما في ذلك plugins

وفي هذه المذكرة، تم تقديم دراسة حول Nagios من خلال ثلاثة فصول، حيث تم توضيح كيفية تثبيت وتكوينNagios ، وتوضيح المفاهيم الأساسية المتعلقة بالشبكات والمراقبة. وتم توضيح مكونات Nagiosووظائفها، وكيفية استخدام Nagios في مراقبة الشبكات وإدارة الأخطاء والأعطال وإنشاء التقارير.

وأخيرًا، يمكن القول أن Nagios هي أداة مفيدة وضرورية للمساعدة في مراقبة وإدارة الشبكات بشكل فعال. وتساعد هذه الأداة الشركات والمؤسسات في الحفاظ على أداء شبكاتها والتعرف على المشكلات في وقت مبكر وحلها قبل أن تؤثر على الأعمال .

المراجع

المراجع

1- http://www.o000o.org/monitoring/bases.html« Etude des outils de surveillance (monitoring) réseau »**,** consulté le 04.06.2023

2- **https://www.monitoring-fr.org/supervision/html**« Communauté Francophone de la Supervision Libre », **consultéle 04.06.2023**

3- **http://ram-0000.developpez.com/tutoriels/reseau/SNMP/«** Présentation du protocole SNMP », **consultéle 04.06.2023**

4- **https://doc.ubuntu-fr.org/virtualbox,**« Virtual box [Wiki ubuntu-fr] »,**consulté le 04.06.2023**

5- **https://www.memoireonline.com/04/12/5604/m_Monitoring-dune-infrastructure-informatique-sur-base-doutils-libres.htm«** Monitoring d'une infrastructure informatique sur base d'outils libres » ,**consulté le 05.06.2023**

6- **https://docplayer.fr/3007113-La-supervision-avec-nagios.html «** La supervision avec NAGIOS - PDF Téléchargement Gratuit (docplayer.fr) »**, consulté le 04.06.2023**

7- **Trabelsi, A. « *Mise en place d'un outil de supervision système et réseau open source* » , Année Universitaire 2014-2015, Mémoire de Mastère Professionnel. Université Virtuelle de Tunis . https://docplayer.fr/48501806-Mise-en-place-d-un-outil-de-supervision-systeme-et-reseau-open-source.html**

8- **Jean G., '*Nagios 3 pour la supervision et la métrologie* : Déploiement, configuration et optimisation', Eyrolles, 2009, pp 32-51. ISBN : 978-2-212-1247**.

9- **Olivier JAN., '*Nagios au cœur de la supervision Open source*'**

2008 ,pp ISBN 978-2-7460-4603-0

10- **https://ar.wikipedia.org//wiki/تيليجرام, « تيليجرام – ويكيبيديا », consulté le 05.06.2023**