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 :

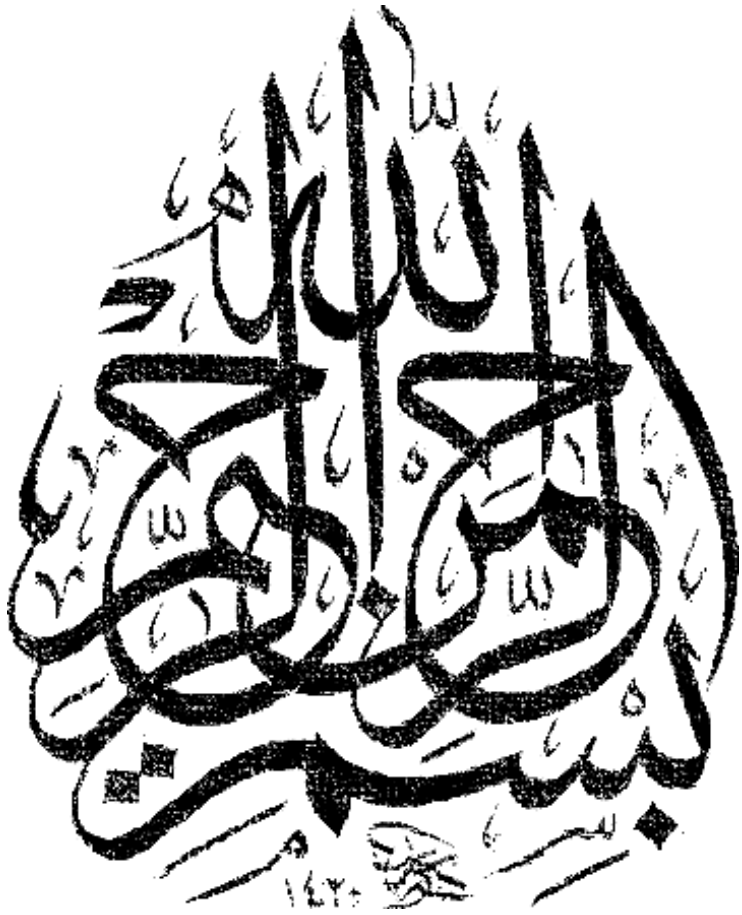
- ***بن والي مليسة اناس***
- ***رباح خيرة***

إعداد أداة مراقبة الشبكة زابيكس

تم الإعلان العلني بتاريخ 06 / 06 / 2024 في تيارت أمام لجنة التحكيم المكونة من:

دحماني يوسف	**الرتبة أستاذ جامعي**	**المشرف**
عالم عبد القادر	**الرتبة أستاذ مساعد أ**	**الرئيس**
العايش فاطمة	**الرتبة أستاذة مساعدة أ**	**المناقشة**

2024-2023


بسم الله الرحمن الرحيم
١٤٢٠

شكر وعرفان

قال تعالى:﴿ لئن شكرتم لأزيدنكم ﴾

نحمد الله الذي يضيء طريقنا ويمنحنا الصبر، ونحمده على نعمة العلم التي منحنا إياها. نشكر الله على المساعدة في إتمام هذا العمل بنجاح، وعلى توجيهه لنا ومساعدته في تجاوز التحديات. ونرفع الصلاة والسلام على خير الأنام،

رسول الله.

لا يجب أن ننسى في هذا السياق أن نعبر عن شكرنا للأستاذ "دحماني يوسف" الذي ساهم أيضًا في بناء جزء كبير من هذا العمل، وقام بإرشادنا خطوة بخطوة منذ البداية وحتى النهاية، ولم يبخل علينا بتوجيهاته ونصائحه.

كما لا ننسى أن نتقدم بالشكر أيضا للأعضاء اللجنة على قبولهم مناقشة هذه المذكرة

كما نشكر كل من ساهم في هذا العمل ومد لنا يد العون من قريب أو بعيد

وفي الأخير نأمل من الله أن يجعل هذا

العمل في ميزان حسناتنا وأن ينتفع منه

كل طالب علم لأنه هدفنا من هذا الانجاز

اهدا

الحمد الله ﷻ والصلاة على الحبيب المصطفى ﷺ

{يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ}

ها انا اليوم اهدي بحثي إلى من أرضعتني لبن الحنان، وسقتني ماء الحياة، إلى من تطيب أيامي بقربها

ويسعد قلبي بهناتها، إلى أعلى كائن في الوجود... أمي

إلى أبي الفاضل الشامخ المكارم والراسخ الفاضل، الحريص علي رؤوف بي رحيم، سندي المتين وأنيسي المعين.

الى اخوتي سندي تميل الدنيا ولا يميلون

إلى رفقاء الدرب الذين كانوا بمثابة إخوة اللهم اهلي احبتي فهم بهم استقيم.

- ✓ مليسة
- ✓ خيرة

الفهرس

مقدمة عامة 1

الفصل الاول: مراقبة الشبكيات وأساسياتها 2

مقدمة 3

1.تعريف نظام مراقبة شبكة الاتصال 3

2.1 أهمية نظام مراقبة شبكة الاتصال 4

2.ما هي مراقبة الخادم؟monitoring server 5

3.مظاهر تأثر أداء الشبكة 5

4. أدوات وبروتوكولات مراقبة الشبكات 5

1.4.الادوات 5

2.4.البروتوكولات 8

3.2.4 بروتوكول إدارة المعلومات العام (CMIP) 10

5.مميزات بروتوكولات مراقبة الشبكات واستخداماتها 10

6.كيف يمكن التأكد من أن نظام مراقبة الشبكة يعمل بشكل جيد؟ 11

7. مزايا مراقبة الشبكات 12

الفصل الثاني: تحليل ومراجعة zabbix في مراقبة الشبكات 14

مقدمة: 15

تاريخ زابيكس: 15

1.تعريف زابيكس "ZABBIX" 17

2.1 أهميته وبماذا يتميز عن غيره 17

2. أنواع برامج لمراقبة شبكات الاتصال 20

3.الايجابيات والسلبيات الزابيكس 23

الخاتمة 23

الفصل الثالث: ضبط وإدارة أداة زابيك 24

مقدمة 25

ماهو VM VirtualBox ؟ 25

1.تثبيت وتكوين زابيكس 26

1.1إنشاء الجهاز الافتراضي الضيف DEBIAN 26

2.1تثبيت خادم قاعدة البياناتMariadb 27
3.1 أوامر تنزيل وتثبيت الحزمة الرئيسية zabbix..... 28
2.تكوين الزابيكس 30
3. مراقبة الشبكة على ويندوز 10..... 33
1.3. تثبيت وكيل زابيكس على ويناوز 10 مُراد مراقبته..... 33
2.3 انشاء المضيف على زابيكس 33
4.تحليل بصري للأداء 34
1.4بعض الرسوم البيانية 35
5.التنبيهات المُرسلة عن طريق زابيكس..... 38
1.5 تكوين زابيكس لإرسال تنبيهات باستخدام تطبيق تليجرام..... 38
2.5. نموذج الرسالة..... 39
3.5 الرسائل المستلمة..... 40
الخاتمة..... 40
خاتمة عامة 42
الملخص 43
المصادر و المراجـع..... 45
الاختصارات 46

فهرس الاشكال:

الشكل 1: مخطط نظام مراقبة شبكة الاتصال..... 4
الشكل 2: مخطط SNMP..... 9
الشكل 3:مخطط ICMP..... 10
الشكل 4: تطورات زابيكس..... 16
الشكل 5:مكونات Zabbix..... 22
الشكل 6:تثبيت Mariadb 27
الشكل 7:واجهة Mariadb 28
الشكل 8:تثبيت مستودع زابيكس..... 29
الشكل 9: تثبيت الوكيل والخادم والواجهة المستخدم..... 30
الشكل 10:عنوان IP الخاص بالخادم الخاص..... 31
الشكل 11: تكوين اتصال قاعدة البيانات..... 31
الشكل 12: ادخال المستخدم 32
الشكل 13:متصفح الويب زابيكس 32
الشكل 14:الوكيل زابيكس 33
الشكل 15: المضيف"hote"..... 34
الشكل 16:العرض بيانات الرصد 35
الشكل 17:رسم بياني وحدة المعالجة المركزية (CPU) 35
الشكل 18:رسم بياني الذاكرة لوينداز 36
الشكل 19:دائرة بيانية مساحة القرص (:c-) OS 36
الشكل 20:دائرة بيانية مساحة القرص(:F)DATA..... 37
الشكل 21:رسم بياني واجهة الشبكة..... 37
الشكل 22:تكوين تطبيق تليجرام..... 39
الشكل 23:صياغة الرسالة..... 39
الشكل 24:الرسائل المستلمة..... 40

مقدمة عامة

مقدمة عامة

في عالم يتسارع فيه التطور التكنولوجي، تظل شبكات الاتصال حيويةً للتفاعل الاجتماعي والتقدم الاقتصادي والابتكار التكنولوجي. تعتبر مراقبة هذه الشبكات مهمة أساسية لضمان استقرارها وسلامة البيانات التي تنقلها. إن فهم أساليب وتقنيات مراقبة شبكات الاتصال وتطويرها بما يتماشى مع تطور التكنولوجيا يمثل تحديًا استراتيجيًا يتطلب المزيد من التحليل والتفكير الاستراتيجي. تمتد أهمية مراقبة شبكات الاتصال بعيدًا عن الجوانب التقنية البسيطة، إلى تأثيرات اقتصادية واجتماعية وسياسية فهي تضمن استمرارية الأعمال وتقديم الخدمات بكفاءة، كما تحمي من التهديدات السيبرانية المتزايدة التي تشكل تهديدًا حقيقيًا على البنية التحتية للاتصالات. هذه المذكرة تهدف إلى استكشاف عمق مراقبة شبكات الاتصال من خلال تحليل التقنيات والأساليب المستخدمة على سبيل المثال، يمكن تطبيق مراقبة شبكة الاتصال باستخدام تطبيق زابيكس، الذي يوفر واجهة رسومية لمراقبة وإدارة الشبكة بشكل فعال .ومن بين التفاصيل الهامة في عمله، يشمل نوع الارسال عبر التلغرام، الذي يسمح بتلقي إشعارات وتحذيرات مباشرة عن حالة الشبكة وأي مشاكل محتملة تتطلب اتخاذ إجراء فوري.

تسعى هذه المذكرة إلى أن تكون مساهمة فعّالة في تطوير مجال مراقبة شبكات الاتصال، وتوفير توجيهات عملية للصناعة والباحثين، بهدف تعزيز أمان الشبكات واستدامة الأعمال في عصر الاتصالات الرقمية.

الفصل الاول:
مراقبة الشبكيات وأساسياتها

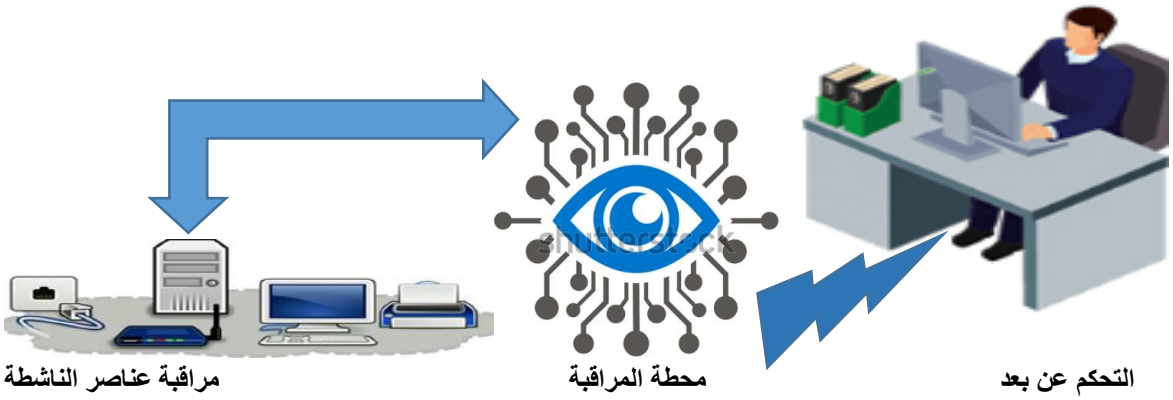
مقدمة:

في لحظة انعدام خدمة الشبكات، سواء بسبب انقطاع في الاتصال أو تعطل في الأجهزة المتصلة بها، نجد أنفسنا محاصرين وعاجزين عن الوصول إلى المعلومات الحيوية في اللحظات الحاسمة. تزيد هذه التجارب من وعينا بالأهمية الكبيرة للشبكات في تسهيل حياتنا اليومية. ومن أجل تجنب مثل هذه المشكلات وللحفاظ على استدامة الاتصالات، يقوم الإنسان بتطبيق مراقبة فعّالة على شبكاته، لفحص ومعالجة الأعطال قبل حدوثها، وللتصدي للتهديدات الأمنية المحتملة. بفضل هذه الإجراءات، يمكن للمؤسسات والأفراد أن يحظوا ببيئة شبكات آمنة وموثوقة تسهم في تحقيق أهدافهم بكفاءة وثقة.

اذن كيف يمكن لتطبيق مراقبة الشبكات بفعالية أن يسهم في تحسين أداء البنية التحتية للاتصالات وضمان استقرارها، خاصة في ظل التحديات المتزايدة مثل زيادة حجم البيانات، وتعقيد الأنظمة الشبكية، وتزايد التهديدات الأمنية؟".

1.تعريف نظام مراقبة شبكة الاتصال:

يشير مصطلح مراقبة الشبكة إلى جميع البرامج والأنظمة التي تضمن مراقبة كل العمليات ضمن الشبكة. بما في ذلك مراقبة جميع مكونات الشبكة كأجهزة الراوتر والسويتش والجدران النارية والسيرفرات والأنظمة الافتراضية والمكونات الأخرى. إن هدف المراقبة هو البحث عن الأخطاء ومتابعة الأداء والقيام بعمليات التقييم بشكل دائم للحفاظ على إمكانية الوصول وتحسينه بشكل مستمر.[1]



الشكل 1: مخطط نظام شبكة الاتصال

2.1 أهمية نظام مراقبة شبكة الاتصال:

يتسم نظام مراقبة الشبكة بأهمية بالغة من حيث أنه:

1. تساهم عملية مراقبة الشبكة في تحديد المشاكل الموجودة في نظام شبكة المؤسسة، مما يسهل بدوره على نظام الإدارة معالجة المشكلة بوضوح، والبحث عن أفضل الحلول المقترحة الممكنة لمعالجة المشكلة، وضمان سد الثغرة التي تسببت في المشكلة و ضمان عدم تكرار المشكلة.
2. تعامل مع محاولات اختراق الشبكة، واكتشاف أن بعض الموظفين في النظام قد اخترقوا حسابات موظفين آخرين. في هذه الحالة، يقوم النظام بإرسال إنذارات وتحذيرات إلى الخادم، ويقوم مراقب الشبكة باكتشاف التعدي على حسابات الموظفين واختراقها ويعمل على معاقبة المتعدين على حقوق الآخرين، وبالتالي تعزيز حماية نظام الشبكة ومنع التعدي عليه بأي شكل من الأشكال.
3. يتم التعامل مع الأعطال في نظام المراقبة بأسرع وقت ممكن للحفاظ على مستويات الجودة وكفاءة أداء العاملين في الإنتاج، حيث يمكن أن يتعطل النظام بأكمله مما يعطل العمل ويضيع الوقت مما يتسبب في خسائر فادحة للمؤسسة.
4. الكشف عن الفيروسات في أنظمة شبكة المؤسسة والعمل على القضاء عليها. تحديد مصدر الثغرات التي تسببت في دخول الفيروس إلى النظام وسدها.
5. تحديد احتياجات نظام الشبكة واحتياجات المؤسسة بطريقة تحليلية وتفصيلية والسعي لتلبية تلك الاحتياجات، بما يضمن سلاسة سير عمليات الإدارة:

6. الكشف عن أسباب انقطاع الشبكة. خاصةً خلال فترات الذروة، عندما يستهلك عدد كبير من العاملين في المؤسسة جزءًا كبيرًا من حزمة الإنترنت في نفس الوقت، تكون استجابة النظام للأوامر الواردة بطيئة. [2]

2.ما هي مراقبة الخادم؟monitoring server

من خلال تنفيذ أداة مراقبة الخادم، يمكنك تتبع البنية التحتية لتكنولوجيا المعلومات بالكامل بشكل أفضل، والتأكد من أن خوادمك لا تعاني من التوقف. في حالة حدوث توقف، ستعمل أدوات مراقبة الخادم على تنبيهك إلى المشكلات حتى تتمكن من اتخاذ إجراء فوري وتقليل التأثير على المستخدمين، بالإضافة إلى تحديد السبب الجذري للمشكلة لتجنب المزيد من التوقف غير المخطط له. [3]

3.مظاهر تأثر أداء الشبكة :

1. انخفاض سرعة الشبكة.
2. زيادة فترات الانتظار للطباعة أوتسجيل الدخول أو أى جهاز موصول بالشبكة (هذه المشاكل تزيد بزيادة الاجهزة التي تتصل بالشبكة).
3. فقدان البيانات (Packet Loss): يمكن أن يؤدي خلل في الشبكة إلى فقدان بعض البيانات أثناء النقل.
4. مراقبة الشبكة الفعال سينبهك اللحظة التي تنشأ فيها حالة ما, لكي تتمكن من التعامل معها فورا ، و بالتالي خفض و تقليل وقت العطلdown-time في حين أن الربط الشبكي لنظام الرصد يمكن أن يوفر معلومات عن المشاكل، يمكنه أيضا أن يقدم معلومات عن تحسين الشبكة.

4. أدوات وبروتوكولات مراقبة الشبكات:

1.4.الادوات:

الأدوات المستخدمة عادة ما تكون مزيجا من المصادر المفتوحة وهي الادوات التي تكون متاحة للجميع مثال" Nagios، Zabbix، OpenNMS "والبرمجيات المرخصة

هذه الأدوات تكون غيرمجانية مدفوعة الثمن ومملوكة لشركات معينة مثال"
PRTG Network ،SolarWinds Network Performance Monitor
."Cisco Network Assistant ،Monitor

يمكن تقسيم أنواع أدوات مراقبة الشبكات إلى فئتين رئيسيتين هما:

1.أدوات رصد للمكتب Office Monitoring Tools :

هي الاحدث في عالم مراقبة الانترنت والبرمجيات. تمكنك من عمل رصد كامل الشبكة من موقع مركزي مواحد. هذا البرنامج أيضا يسمح لك بتتبع الاجهزة التي يمكن للمستخدمين استعمالها على الشبكة الخاصة بك بسهولة. لأنه يجمع بين spysure remote surveillance و individual user monitoring فهو الاشمل في مراقبة الشبكة . بالاظافة الى أن جميع كلمات السر الخاصة بك محمية عن طريق التشفير encryption على الإنترنت.

2. أدوات رصد للأنترنت Internet Monitoring Tools:

نوع من البرمجيات التي تستحوذ وتسجل جميع الأنشطة القائمة على الإنترنت والتي يمكن للمستخدم على جهاز الكمبيوتر الخاص بك تحقيقها. الإجراءات المسجلة مثل: زيارات الموقع، محادثات الدردشة عبر الإنترنت ، والرسائل المرسله عبر البريد الإلكتروني على الويب ، و الصور المعروضة ، وغير ذلك الكثير. ببساطة أرسل تهيئه وحدة المراقبة للمكاتب الخاصة بك لأجهزة الكمبيوتر عن بعد. على المستخدم فقط تشغيل الملفات الخاصة ولن يعلموا أنهم يجري رصدهم.

Remote Monitoring and Management"

---

spysure remote surveillance تشير المراقبة والإدارة عن بعد (RMM) إلى جميع الحلول البرمجية لمراقبة أنظمة الكمبيوتر والتحكم فيها عن بعد (مثل محطات العمل أو الخوادم أو أجهزة الكمبيوتر الأخرى المتصلة).

1.1.4 أنواع الأدوات مراقبة الشبكات:

تتمثل أنواع أدوات مراقبة الشبكات في العديد من التصنيفات الرئيسية التي تشمل الأدوات التالية:

1. **أدوات الرصد (Monitoring Tools):**
   - تُستخدم لمراقبة حالة الشبكة والأنظمة عبر الشبكة بشكل مستمر.
   - تتضمن قياسات أداء الشبكة وتوافر الخدمات واستخدام الموارد وغيرها.
   - مثال ipMonitor devoloper par solar wind
2. **أدوات تحليل حركة البيانات (Traffic Analysis Tools):**
   - تسمح بتحليل حركة البيانات عبر الشبكة لفهم الأنماط والاستخدام وتحديد المشكلات.
   - يمكن استخدامها لاكتشاف انخفاض أداء الشبكة وتحديد أسبابه.
   - مثال ActiveXperts Network Monitor.

t un outil de surveillance et de gestion de réseaux développé par ActiveXperts Software.

3. **أدوات إدارة التكوين (Configuration Management Tools):**
   - تُستخدم لإدارة تكوينات الأجهزة والخوادم والتطبيقات عبر الشبكة.
   - تهدف إلى ضمان أمان التكوينات والتوافق مع المعايير.

4. **أدوات الأمان والتحليل الأمني (Security and Analysis Tools):**
   - تستخدم لرصد الأمان عبر الشبكة وتحليل السجلات وكشف التهديدات.
   - تساعد في تقديم تقارير حول الثغرات الأمنية والأنشطة غير المشروعة.

5. **أدوات تحسين الأداء (Performance Optimization Tools):**
   - تستخدم لتحسين أداء الشبكة والتطبيقات وتحسين استخدام الموارد.
   - تقدم تحليلاً وتوصيات لتحسين أداء الشبكة.

هذه الأدوات تعمل معًا لضمان سلامة وأمان وأداء موثوق بها للشبكات والأنظمة المختلفة

2.4.البروتوكولات:

بما أن وظائف مراقبة الشبكة هي الوظائف الأساسية التي تعتمد عليها جميع انظمة إدارة الشبكات وبروتوكولاتها؛ لذلك لا يمكن الحديث عن بروتوكولات المراقبة من دون الحديث عن بروتوكولات إدارة الشبكات. هناك العديد من هذه البروتوكولات والتي تعمل على تنفيذ بعض الوظائف المحددة بالنموذج او جميعها من أشهر هذه البروتوكولات: (SNMP/NETFLOW / CMIP)

implementer par udp

1.2.4بروتوكول إدارة الشبكات البسيط (SNMP):

هو بروتوكول اتصال يسمح لنا بمراقبة تجهيزات الشبكة التي نديرها، مثل الموجّهات والخوادم والطابعات وأجهزة أخرى عاملة ببروتوكول IP جميعًا ضمن نظام أو برمجية إدارة واحدة؛ وإذا كان جهاز الشبكة يدعم بروتوكول SNMP، يمكننا تفعيله وإعداده لجمع المعلومات ومراقبة عدة تجهيزات شبكية من نقطةٍ واحدة. مكونات SNMP تتألف من :

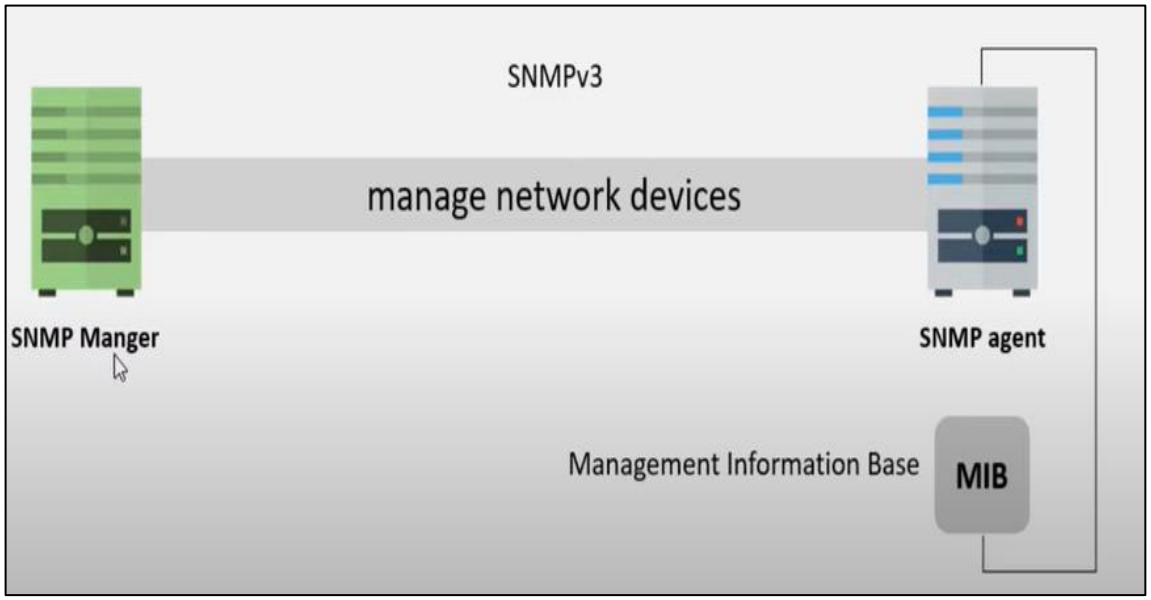
مكونات SNMP تتضمن مدير SNMP، أجهزة مُدارة مع وكيل SNMP، و MIB SNMP تحتوي على OID SNMP.

- مدير SNMP: النظام المركزي لمراقبة شبكة SNMP، يعرف أيضًا بمحطة إدارة الشبكة (NMS)، ويتواصل مع الأجهزة عبر وكيل SNMP لجمع البيانات واستلام الأحداث.
- الأجهزة المُدارة: كيانات شبكية متوافقة مع SNMP مثل الموجهات، مفاتيح التبديل، الطابعات، والأجهزة اللاسلكية، تُدار بواسطة مدير SNMP.
- وكيل SNMP: برنامج على الجهاز الشبكي يستجيب لطلبات مدير SNMP، يوفر حالة الجهاز وإحصائياته.
- MIB SNMP: هيكل يحدد تنسيق تبادل المعلومات في SNMP، يدير وكيل SNMP قاعدة بيانات لمعلومات الجهاز، وتُخزّن البيانات المجمعة بواسطة مدير SNMP في MIB.

nombreuses MIB définies par des organismes de normalisation tels que l'IETF et l'ISO

Les ports SNMP sont utilisés via UDP 161 pour les gestionnaires SNMP communiquant avec les agents SNMP (c'est-à-dire interrogation) et UDP 162 lorsque les agents envoient des interruptions non sollicitées au gestionnaire SNMP.

-OID SNMP: معرفات كائنات تُحدد بسلاسل أرقام مفصولة بنقاط، تنظمها MIB في هيكل شجري .[6] (OID) est un identifiant MIB utilisé pour délimiter les appareils au sein de la MIB



الشكل 2: مخطط SNMP

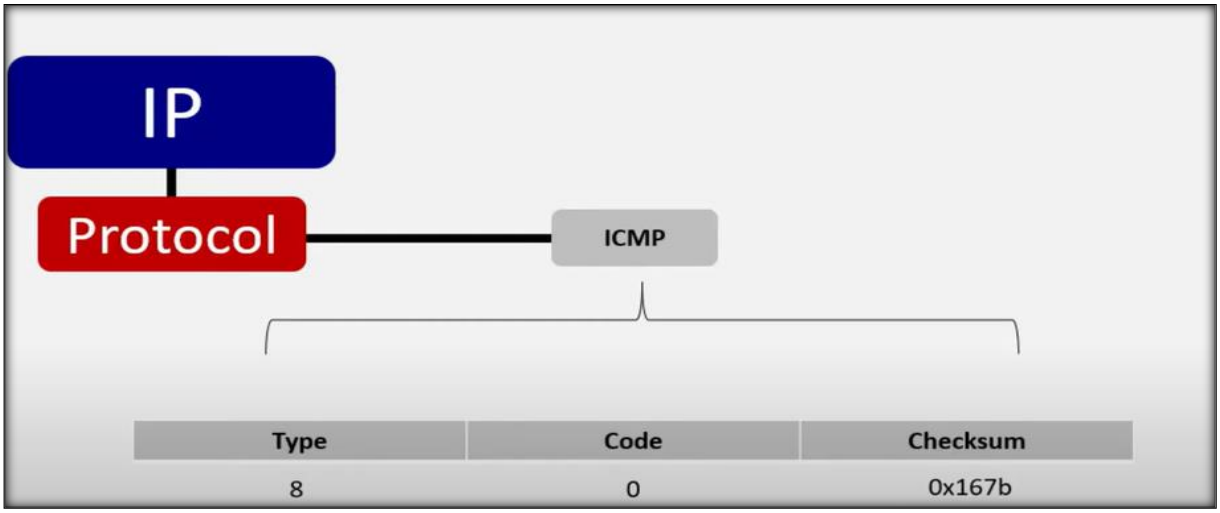
2.2.4 بروتوكولNetFlow :

النتفلو هو بروتوكول شبكي تم تطويره من قبل شركة سيسكو لجمع معلومات حركة المرور عبر البروتوكول الإنترنت (IP) ومراقبة تدفق الشبكة. من خلال تحليل بيانات النتفلو، يمكنك الحصول على صورة عن تدفق وحجم حركة المرور في الشبكة.

هو تقنية من اتجاه واحد، لذا عندما يستجيب الخادم لطلب العميل الأولي، يعمل العملية بالاتجاه المعاكس وينشئ سجل تدفق جديد. باستخدام حلول مراقبة النتفلو، يمكنك مراقبة وتحليل هذه السجلات بشكل أكثر كفاءة وفعالية لحركة المرور داخل الشبكة[7] .

3.2.4 بروتوكول إدارة المعلومات العام (CMIP):

هو بروتوكول الطبقة 3 من نموذج OSI يعوض غياب رسائل الخطأ في بروتوكول IP(بروتوكول الإنترنت). في الواقع، في حالة وقوع حادث إرسال، ستستخدم المعدات الوسيطة هذا البروتوكول لإخطار جهاز الإرسال. إنه بروتوكول بسيط جدًا، وليس له وظيفة مباشرة لمراقبة الشبكة ولكنه يستخدم كمصدر معلومات حول جودة الشبكة أو حول وجود جهاز.



الشكل 3:مخطط ICMP

5.مميزات بروتوكولات مراقبة الشبكات واستخداماتها:

تُعدّ بروتوكولات مراقبة الشبكات ونظمها من الأدوات الأساسية لمديري الشبكات الحاسوبية، والتي توفر لهم مؤشرات عن الحالة الصحية للشبكة ومكوناتها، لضمان استمرارها في العمل على النحو الأفضل. تتميز بروتوكولات مراقبة الشبكات ونظمها عموماً بتوفير المزايا التالية:

- مراقبة أداء كل مكون من مكونات الشبكة وتوفير المعلومات والمؤشرات والإنذارات في حال حدوث طارئ في أي مكوّن من مكونات الشبكة ليصل إلى معالجته في الوقت المناسب.

- مراقبة الأخطاء والأسباب الناجمة عنها لاتخاذ التدابير اللازمة.
- مراقبة تدفق المعلومات في خطوط الشبكة والتنبؤ بأماكن الاختناقات لمعالجة الحالة قبل حدوثها.
- مراقبة حسابات المستثمرين في الشبكة.
- مراقبة التطبيقات المختلفة على المخدمات وسلامة استخداماتها.
- مراقبة الثغرات الأمنية التي قد توجد ضمن الشبكة لاتخاذ الإجراءات المناسبة

6.كيف يمكن التأكد من أن نظام مراقبة الشبكة يعمل بشكل جيد؟

في البداية يجب أن تقوم بتحديد كل الأجهزة ومعاينة الأداء الخاص بها. ومن ثم تحديد الأمور والنقاط المهمة التي يجب العمل على مراقبتها. أما الخطوة التالية ستكون البدء بعمليات المراقبة والتي ستكون مختلفة بحسب نوع الجهاز الذي ستطبق عملية المراقبة عليه. وهنا يجب أن يتم تحديد الأولويات. مثلاً إن مراقبة أجهزة سطح المكتب والطابعات ليس بنفس أهمية مراقبة السيرفرات وأجهزة التوجيه (الراوتر) وأجهزة السويتش كون هذه الأجهزة لها الدور الأهم في العمل وأي خلل أو عطل فيها سيكون له تأثير سلبي كبير على كامل أداء الشبكة، باختصار للحصول على مراقبة فعالة للشبكة، تحتاج إلى:

- ✓ تحسين الفاصل الزمني للرصد
- ✓ اختيار البروتوكول الصحيح
- ✓ مراقبة الأساسيات فقط
- ✓ تحديد العتبات

7. مزايا مراقبة الشبكات:

تنطوي مراقبة الشبكة على عدد من الفوائد المهمة والضرورية، بما في ذلك:

1. **تحسين أداء الشبكة:** من خلال الفحص المنتظم لحركة المرور وأداء الشبكة، يمكن لمراقبة الشبكة تحديد العوامل التي تؤثر على أداء الشبكة واتخاذ إجراءات علاجية لتقليل انقطاع الاتصال والسرعة والاستقرار، وتحسين السرعة والاستقرار.
2. **الكشف المبكر عن المشاكل:** تتيح مراقبة الشبكة الاكتشاف المبكر لأعطال الشبكة ومشاكلها قبل أن تؤثر سلباً على أداء النظام بشكل عام، مما يقلل من وقت التعطل والتكاليف المرتبطة باستكشاف الأعطال وإصلاحها.
3. **تحسين الأمن السيبراني:** من خلال مراقبة نشاط الشبكة، يمكن الكشف بسرعة عن النشاط غير المصرح به والهجمات السيبرانية المحتملة واتخاذ التدابير الوقائية المناسبة، مما يقلل من مخاطر الاختراق وفقدان البيانات.
4. **حسن إدارة السعة:** تراقب مراقبة الشبكة استخدام النطاق الترددي وتخصيص السعة بين الأجهزة والتطبيقات لتحسين استخدام الموارد وتجنب ازدحام الشبكة.
5. **توفير تقارير وإحصائيات دقيقة:** يمكن لأنظمة مراقبة الشبكة إنشاء تقارير منتظمة تُظهر أداء الشبكة واستهلاك الموارد وأنماط الاستخدام، مما يمكّن مديري الشبكة من اتخاذ قرارات مستنيرة بناءً على بيانات دقيقة وموثوقة توفير إحصائيات.

8.التحديات مراقبة الشبكات :

تواجه مراقبة الشبكات تحديات كبيرة نتيجة لزيادة حجم البيانات وتعقيد البيئات الشبكية المعاصرة. تشمل هذه التحديات الحاجة إلى:

1. **زيادة حجم البيانات وتعقيد الشبكات:** مع زيادة حجم البيانات وتعقيد الشبكات، يمكن أن تواجه تحديات في تحليل البيانات واكتشاف الأنماط غير العادية. للتغلب على هذا التحدي، يجب تطبيق تقنيات الذكاء الاصطناعي وتحليل البيانات الكبيرة لمعالجة البيانات بشكل فعال وتحديد الأنماط المهمة.

2. **أمن المعلومات والخصوصية**: تحمل مراقبة الشبكات مسؤولية كبيرة في حماية البيانات وضمان سرية المعلومات. ومن اجل تفادي ذلك يجب تطبيق أفضل الممارسات في أمن المعلومات واستخدام تقنيات التشفير ومراقبة الوصول بشكل دقيق.
3. **تكاليف التشغيل والصيانة:** قد تكون تكاليف تشغيل وصيانة أنظمة مراقبة الشبكات باهظة الثمن، خاصة مع تزايد تعقيد الشبكات وزيادة حجم البيانات. لذاك يمكن استخدام الحلول السحابية والتحليل الذكي لتحسين كفاءة التكاليف والأداء.
4. **التوافق والتكامل:** قد يكون التوافق والتكامل بين أنظمة مراقبة الشبكات المختلفة تحديًا، خاصة عند استخدام تقنيات متنوعة. يجب التركيز على استخدام حلول متكاملة وتوفير واجهات برمجة تطبيقات (APIs) للتكامل السلس بين الأنظمة المختلفة.
5. **تحديات التشخيص والاستجابة السريعة:** يجب أن تكون عمليات التشخيص والاستجابة سريعة وفعالة لمعالجة المشكلات في الشبكة بسرعة. يمكن استخدام تطبيقات الذكاء الاصطناعي والتحليل التنبؤ لتحديد المشكلات المحتملة مبكرًا واتخاذ الإجراءات اللازمة بشكل فوري.

الخاتمة

إن مراقبة الخوادم تعتبر ممارسة أساسية لضمان توافر الخدمات الحاسوبية بشكل مستمر، واستقرار الأنظمة، ورضا المستخدمين. من خلال مراقبة الأداء والموارد وسلامة الخوادم بشكل مستمر، يمكن لفرق تكنولوجيا المعلومات اكتشاف وحل المشكلات المحتملة بسرعة قبل أن تؤدي إلى اضطرابات في العمليات التجارية. بالإضافة إلى ذلك، تسمح المراقبة النشطة بتحسين استخدام الموارد، وزيادة الكفاءة التشغيلية، وضمان تجربة مستخدم مثلى. عبر دمج أدوات المراقبة المتقدمة وممارسات إدارة الحوادث، يمكن للمؤسسات تعزيز موثوقية وأمان بنيتها التحتية الحاسوبية. في النهاية، يُعتبر الاستثمار في مراقبة الخوادم عنصرًا أساسيًا في أي استراتيجية حاسوبية قوية وموجهة نحو الأداء.

الفصل الثاني:

تحليل ومراجعة **zabbix** في مراقبة الشبكات

مقدمة:

في العصر الحالي، تتحرك البيانات بسرعة الضوء، حيث كانت الجودة في الثمانينيات هي هدفنا الأسمى، ولكن مع تغير العصر والثورة التكنولوجية الجذرية في الثلاثينيات الأخيرة، تبدلت الأولويات بشكل كبير، وهذا ما جعل عصرنا يُسَمَّى عصر السرعة.لكي تكون شبكات المؤسسات الحديثة فعالة، يجب أن تكون قادرة على دعم مجموعة واسعة من التطبيقات والبروتوكولات والخدمات. تتميز هذه الشبكات بأربع خصائص أساسية: بنية العمل، وتحمل الأخطاء، وقابلية التوسع، وجودة الخدمة، بالإضافة إلى الأمان.

عدم القدرة على تحقيق هذه الخصائص الأساسية يمكن أن يؤدي إلى تعطيل "الجهاز العصبي الرقمي" بأكمله للشركة، مما يتسبب في تراكم جميع العمليات الداخلية.من أجل تحقيق هذه الخصائص الأساسية للشبكة، يجب تصميم البنية التحتية لتكنولوجيا المعلومات والاتصالات. ومع ذلك، فإن تحقيق هذه الأهداف ليس بالأمر السهل، حتى في الشبكات المتقدمة. لذا، يتعين عليها مراقبة هذه المشاكل لضمان القدرة على الرد والاستجابة بسرعة.

ومن أجل مراقبة الشبكات، قام الإنسان بتطوير العديد من الأدوات لمراقبة ورصد الشبكات، من بينها ما سنتطرق إليه في هذا الفصل: "برنامج Zabbix". سنتحدث عن مفهوم برنامج المراقبة زابيكس، والهدف منه، وكيفية عمله، بدءًا من تاريخه ونظرة عامة عنه، بالإضافة إلى مناقشة مميزاته وإيجابياته وسلبيات.

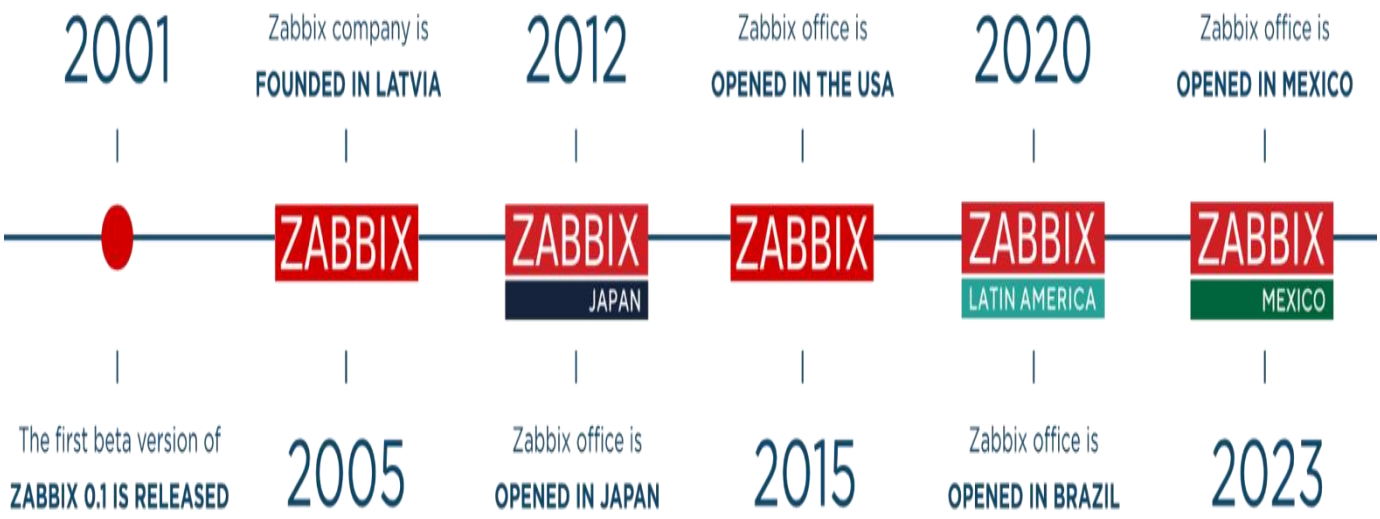
تاريخ زابيكس:

يعود تاريخ برنامج زابيكس إلى عام 1998، حيث نشأ كفكرة شخصية لألكسي فلاديشيف، الذي كان في ذلك الوقت يعمل كمسؤول لإدارة قواعد البيانات في إحدى البنوك. في إطار تلك الفترة، ومن خلال الحاجة لتسهيل العمليات الروتينية، بدأ فلاديشيف في تطوير النسخة الأولى من زابيكس، والتي كانت تعتمد على لغة برمجة بيرل. بعد ثلاث سنوات من

العمل الجاد، تم إصدار أول نسخة عامة من زابيكس في عام 2001 تحت اسم Zabbix v1.0 alpha 1وفقًا لترخيص.GPL

منذ ذلك الحين، حقق زابيكس شهرة واسعة، حيث تم تثبيته في أكثر من 500,000 شبكة فقط في عام 2013، كما تحصل مؤخرًا على العديد من الجوائز والتصنيفات الإيجابية من قبل جهات النشر الموثوقة. يُعتبر زابيكس اليوم مهمًا في سوق حلول الشبكات، نظرًا لقدرته على دعم مجموعة واسعة من التطبيقات والخدمات.لحلول زابيكس العديد من الميزات المبتكرة، مثل الاكتشاف التلقائي الذي يساعد في العثور على عناصر الشبكة بشكل آلي وإضافتها تلقائيًا.

يتمتع زابيكس بدعم مستمر وتحديثات منتظمة، حيث من المتوقع إصدار النسخة الطويلة الأمد القادمة، زابيكس 3.0، في مايو أو يونيو 2015، مما يؤكد التزامه بتقديم أحدث التقنيات والميزات لمستخدميه.ويتم حاليًا تطويره ودعمه بشكل نشط بواسطة ZABBIX SIA.لذا يمكن القول بانه مادام مستمر بالتطور سيبقا متقدم عن غيره.



الشكل 4: تطورات زابيكس

1.تعريف زابيكس "ZABBIX" :

زابكس هو حل مفتوح المصدر على مستوى المؤسسة لمراقبة الشبكات الموزعة .زابكس هو برنامج يراقب العديد من معايير الشبكة وصحة وسلامة الخوادم، الآلات الافتراضية، التطبيقات، الخدمات، قواعد البيانات، المواقع الإلكترونية، السحابة وأكثر من ذلك. يستخدم زابكس آلية إشعارات مرنة تسمح للمستخدمين بتكوين تنبيهات عبر البريد الإلكتروني لأي حدث تقريبًا. هذا يسمح برد فعل سريع على مشاكل الخادم. يوفر زابكس ميزات ممتازة لإعداد التقارير وتصور البيانات بناءً على البيانات المخزنة. هذا يجعل زابكس مثاليًا لتخطيط السعة .يدعم زابكس كلا من الاستقصاء والتقاط البيانات. يتم الوصول إلى جميع تقارير وإحصائيات زابكس، بالإضافة إلى معلمات التكوين، من خلال واجهة أمامية مستندة إلى الويب. تضمن الواجهة الأمامية المستندة إلى الويب أنه يمكن تقييم حالة شبكتك وصحة خوادمك من أي موقع. إذا تم تكوينه بشكل صحيح، يمكن أن يلعب زابكس دورًا هامًا في مراقبة البنية التحتية لتكنولوجيا المعلومات. هذا صحيح على حد سواء بالنسبة للمنظمات الصغيرة التي لديها عدد قليل من الخوادم وللشركات الكبيرة التي لديها العديد من الخوادم.[9]

2.1 أهميته وبماذا يتميز عن غيره:

يمثل زابيكس الحل الشامل والفعّال لمراقبة وإدارة الشبكات، مما يضعه في مقدمة الحلول المتقدمة في هذا المجال. يتميز زابيكس بعدة جوانب عن منافسيه وتجعله اختيارًا ممتازًا للشركات التي ترغب في تحقيق الكفاءة والتميز في إدارة بنيتها التحتية للشبكة.

1. يبدأ تلقائيًا في اكتشاف الشبكة التي تقع تحت رادار عملاء زابيكس .
2. يقوم زابيكس بدعم الوكيل المعتمد وغير الوكيل، مما يتيح له مراقبة شاملة وشخصية لجميع عناصر الشبكة بدقة وفعالية لا مثيل لها.

3. يتمتع زابيكس بقدرة استثنائية على مراقبة أداء الشبكة وتوفرها، وذلك بفضل تحليله الشامل والمتقدم للبيانات ودعمه الكامل لبروتوكولSNMP ، مما يجعله على استعداد دائم للتصدي لأي تحدي يواجه بنية الشبكة.
4. الكشف تلقائيًا عن تغييرات تكوين الجهاز.
5. يقدم زابيكس دعمًا متفوقًا لبرامجVMware ، مما يسهل على المستخدمين رصد وإدارة بيئات الحوسبة السحابية والتقنيات الظاهرية بكفاءة واحترافية عالية.

يتميز زابيكس بنظام إنذار فعّال ومتطور يضمن رصدًا دائمًا لحالة الشبكة وتنبيه المسؤولين في حالة وجود أي مشكلة، مما يضمن الاستجابة السريعة والفعالة وتصحيح المشكلات قبل أن تؤثر على أداء الخدمات وسير العمل بالشرك.

بفضل هذه الخصائص الفريدة والقدرات الاستثنائية، يعد زابيكس الخيار الأمثل للشركات التي تسعى إلى تحقيق التميز والكفاءة في إدارة شبكاتها، ويمثل ركيزة أساسية لضمان استمرارية الأعمال وتحقيق النجاح في البيئة التقنية المعاصرة.

fournir des ressources informatiques à la demande sur Internet avec une tarification au coût par utilisation.

ميزاته:

زابيكس هو حل متكامل لمراقبة الشبكات، يوفر مجموعة متعددة من الميزات في حزمة واحدة:

- ✓ **جمع البيانات:**
- فحوصات الأداء والتوافر
- دعم بروتوكولات SNMP (كلا من الاصطياد والاستطلاع)، IPMI، JMX،
- فحوصات مخصصة
- جمع البيانات المطلوبة على فترات زمنية مخصصة
- يتم التنفيذ بواسطة الخادم/البروكسي وبرامج الوكيل

on peut definier les seuille

✓ **تعريفات عتبات مرنة**

• يمكنك تعريف عتبات مشكلة مرنة للغاية، تسمى المُشغلات، تشير إلى القيم من قاعدة بيانات الخلفية

✓ **إنذارات قابلة للتكوين بشكل مرن**

• يمكن تخصيص إرسال الإشعارات بما يتماشى مع جدول التصعيد والمستلم ونوع الوسائط
• يمكن جعل الإشعارات ذات معنى ومفيدة باستخدام متغيرات البديلة
• تشمل الإجراءات التلقائية الأوامر عن بُعد

✓ **رسم بياني في الوقت الحقيقي**

• يتم رسم العناصر المراقبة على الفور باستخدام وظيفية الرسم البياني المضمنة

✓ **قدرات مراقبة الويب**

• يمكن لزابيكس اتباع مسار من النقرات المحاكاة للفأرة على موقع ويب والتحقق من الوظائف ووقت الاستجابة

✓ **خيارات العرض الشامل**

• القدرة على إنشاء رسوم بيانية مخصصة يمكن أن تجمع عدة عناصر في عرض واحد
• خرائط الشبكة
• التقارير

✓ **تكوين سهل**

• إضافة الأجهزة المراقبة كنظير عامل (host)
• يتم التقاط النظراء العاملين للمراقبة، بمجرد إضافتهم إلى قاعدة البيانات
• تطبيق القوالب على الأجهزة المراقبة

✓ **واجهة ويب سريعة**

- واجهة أمامية قائمة على الويب بلغة PHP
- يمكن الوصول إليها من أي مكان
- يمكنك النقر للتنقل من خلالها
- سجل تدقيق

2. أنواع برامج لمراقبة شبكات الاتصال :

هناك العديد من ادوات مراقبة الخادم لكل منها مميزات ومزايا تميزه عن غيره نذكر منها :

- **ناجيوس كور(NAGIOS CORE):** نظام مفتوح المصدر لمراقبة البنية التحتية للتقنية المعلوماتية. يتيح لك مراقبة أجهزة الاستضافة (الخوادم، المقسمات، الطابعات، إلخ) والخدمات (العمليات، التطبيقات، السجلات، إلخ) على شبكة IP.

- **الدوت كوم مونيتور (.com monitor):** خدمة لمراقبة مواقع الويب والخوادم. تتيح لك مراقبة توفر مواقعك الإلكترونية وخوادمك وواجهات برمجة التطبيقات وغيرها من المصادر، فضلاً عن مراقبة أوقات استجابتها وأدائها من عدة مواقع حول العالم.

- **مراقب شبكة (PRTG Network Monitor):** برنامج تجاري لمراقبة الشبكات طورته شركة Paessler AG. يتيح لك مراقبة النطاق الترددي واستخدامه والتطبيقات وخدمات الشبكة وجودة الخدمة والعديد من جوانب أخرى لأنظمة تقنية المعلومات.

ملخصاً، تتيح لك هذه الأدوات مراقبة حالة وأداء وتوفر البنى التحتية والخدمات التقنية لمؤسستك بشكل مركزي

1.2مقارنة بين بعض ادوات المراقبة: [11],[12],[13],[14]

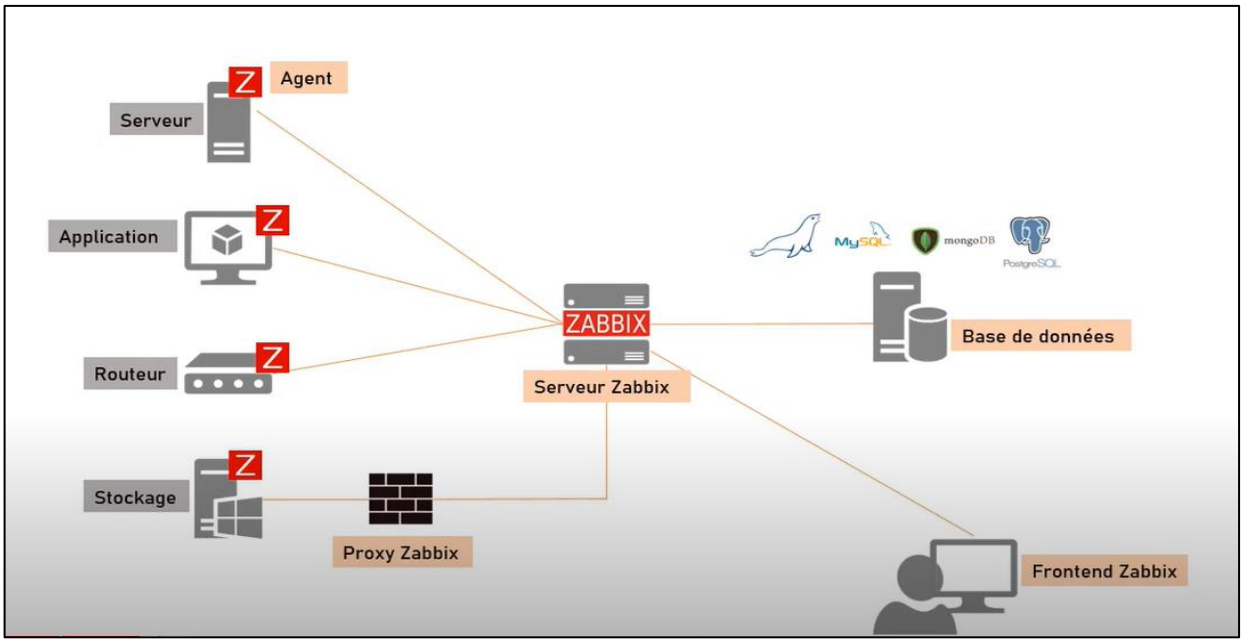
الادوات / الاختلاف	ناجيوس	زابيكس	الدوت كوم مونيتور	مراقب شبكة PRTG
التكلفة	أداة مراقبة خادم مفتوحة المصدر	أداة مراقبة خادم مفتوحة المصدر	هو خدمة تقديمية تُقدم من قبل شركة Dotcom-Monitor اي انه مكلف	تختلف تكلفة PRTG حسب عدة عوامل بما في ذلك عدد الأجهزة المراقبة
امكانية الاستخدام	سهل الاستخدام	سهل الاستخدام	سهل الاستخدام	سهل الاستخدام
كفاءة استهلاك الموارد	يستهلك كميات اقل من الطاقة والموارد مقارنة بالبرامج الأخرى	الذاكرة (RAM) ووحدة المعالجة المركزية (CPU) ومساحة التخزين	يتطلب موارد النظام	يمكن أن تختلف بناءً على حجم الشبكة المراد مراقبتها وتكوينات النظام
الوقت اللازم لاستجابة الاستعلامات و التحديثات	يستجيب على الفور	يستجيب على الفور	يمكن أن يتطلب وقتًا للاستجابة	يختلف إلحاح التنبيه اعتمادا على شدة المشكلة والوقت
نطاق المراقبة	للخوادم والتطبيقات وأجهزة الشبكة	مراقبة البنى التحتية لتكنولوجيا المعلومات الموزعة ، بما في ذلك البيئات السحابية والبنى التحتية الافتراضية.	مراقبة وقت تشغيل موقع الويب ومراقبة تطبيقات الويب ومراقبة الشبكة ومراقبة الخادم	استخدام وحدة المعالجة المركزية ومساحة القرص وحركة مرور الشبكة وأداء التطبيق.

1.1.2 تصميم زابيكس :

كأي نَظام أخر متكامل يتكون نظام زابيكس من عدة مكونات رئيسية لضمان عمله وهي :

1. **الخادم "Zabbix Server"**: يمثل قلب نظام زابيكس، حيث يتم تنصيبه على الخادم الرئيسي ليقوم بمهام المراقبة وجمع البيانات من وكلاء الشبكة وكلاء زابيكس والعملاء الآخر

2. **Zabbix Proxy:** عمل كوكيل للقيام بجمع البيانات من الأجهزة الموجودة في بيئات شبكية بعيدة عن الخادم الرئيسي. يساعد الوكيل الخادم الرئيسي في تقليل الضغط عليه وتحسين أداء النظام.
3. **Zabbix Agent:** يعتبر وكيل زابيكس الواجهة الرئيسية بين الخادم وأجهزة المراقبة. يقوم بتثبيته على الأجهزة المراد مراقبتها ويقوم بجمع البيانات المتعلقة بالأداء والصحة وإرسالها إلى الخادم للتحليل.
4. **واجهة الويبGUI :** تمثل البوابة الرئيسية للتفاعل مع نظام المراقبة،فهي واجهة مستخدم رسومية سهلة الاستخدام وفعّالة لإدارة النظام وعرض البيانات المراقبة. تساعد هذه الواجهة المستخدمين على متابعة أداء النظام بسهولة وتحليل البيانات بشكل دقيق، مما يسهل اتخاذ القرارات السريعة والفعّالة لتحسين أداء الشبكة وضمان استقرارها.
5. **وسائط الخادم Media Server :**الخادم مسؤول عن إرسال إشعار التنبيه عبر البريد الإلكتروني والرسائل النصية القصيرة أثناء استخدام قاعدة البيانات
6. **قاعدة البيانات Database:**يتم فيها تخزين جميع بيانات المراقبة وتحليلها واسترجاعها. [15]



الشكل 5:مكونات Zabbix

3.الايجابيات والسلبيات الزابيكس:

❖ الايجابيات

- باقة Zabbix متاحة بدون أي رسوم على الإطلاق.
- يستخدم المطورون أداة مراقبة تطبيق Zabbix لمراقبة خادم البيانات.
- اداة مراقبة شبكة مضمونة تلبي تمامًا متطلبات أي شبكة مهما كان الحجم.
- يمكنك تقليل ضجيج الإشعارات باستخدام ميزة ارتباط الأحداث.
- لديها تطبيق الهاتف "ارسائل القصيرة ,التليغرام ,فيسبوك .."
- يمكنك تشغيل الاوامر عن بعد .

❖ السلبيات

- لا تتوفر خيارات الدعم
- لا يدعم التنبؤ بالاتجاه. لم يتم تضمين هذه الميزة من قبل فريق Zabbix لأنها تقلل من الأداء العام
- التنقل الحالي للواجهة الأمامية معقد للغاية
- المعلومات مقطوعة. أي انه إذا كان المستخدمون يرغبون في رؤية رسم بياني لعنصر ما، فيجب عليهم الانتقال إلى مكان آخر.

الخاتمة

باختصار، تحليل ومراجعة زابيكس في مراقبة الشبكات تسلط الضوء على أهمية استخدام زابيكس كأداة قوية وفعالة في مجال مراقبة الشبكات. من خلال فحص وتقييم أداء زابيكس ومقارنته بالأدوات الأخرى، يمكننا فهم الفوائد والمزايا التي يقدمها هذا البرنامج للمستخدمين. بفضل قدراته المتعددة وواجهته السهلة الاستخدام، يمكن لـ زابيكس أن يكون حلاً شاملاً لمتطلبات مراقبة الشبكات في البيئات المعقدة. تحليل ومراجعة زابيكس في مراقبة الشبكات تبرز أهمية اعتماد التقنيات الحديثة لضمان أمن واستقرار البنية التحتية للشبكات، وتشير إلى أن زابيكس هو أداة قوية وموثوقة لتلبية هذه الاحتياجات.

الفصل الثالث:

ضبط وإدارة أداة زابيك

مقدمة

في هذا الفصل، سنركز على عملية تثبيت وتكوين خادم زابيكس وواجهته الويب عبر دبيان 12 الذي تم تثبيته على VM Virtualbox وكذلك سنتناول تثبيت وكيله المسمى بـ zabbix-agentعبر الجهاز الفعلي لجهاز الكمبيوتر الشخصي الذي يعمل بنظام التشغيل Windowsالمراد مراقبته ويُعتبر زابيكس أداة مهمة في مجال تقنية المعلومات حيث يُستخدم لرصد ومراقبة البنية التحتية للأنظمة والتطبيقات. يتميز زابيكس بالقدرة على جمع البيانات، تحليلها، عرضها على شكل رسوم بيانية، وتخزينها وارسال اشعارات عبر تطبيق التيليقرام في حالة وجود تنبيهات . يأتي زابيكس مع ثلاثة مكونات رئيسية، الخادم والوكيل والواجهة الأمامية، وتثبيت كل منها يتطلب استخدام الحزم الخاصة بها.

ماهو VM VirtualBox ؟

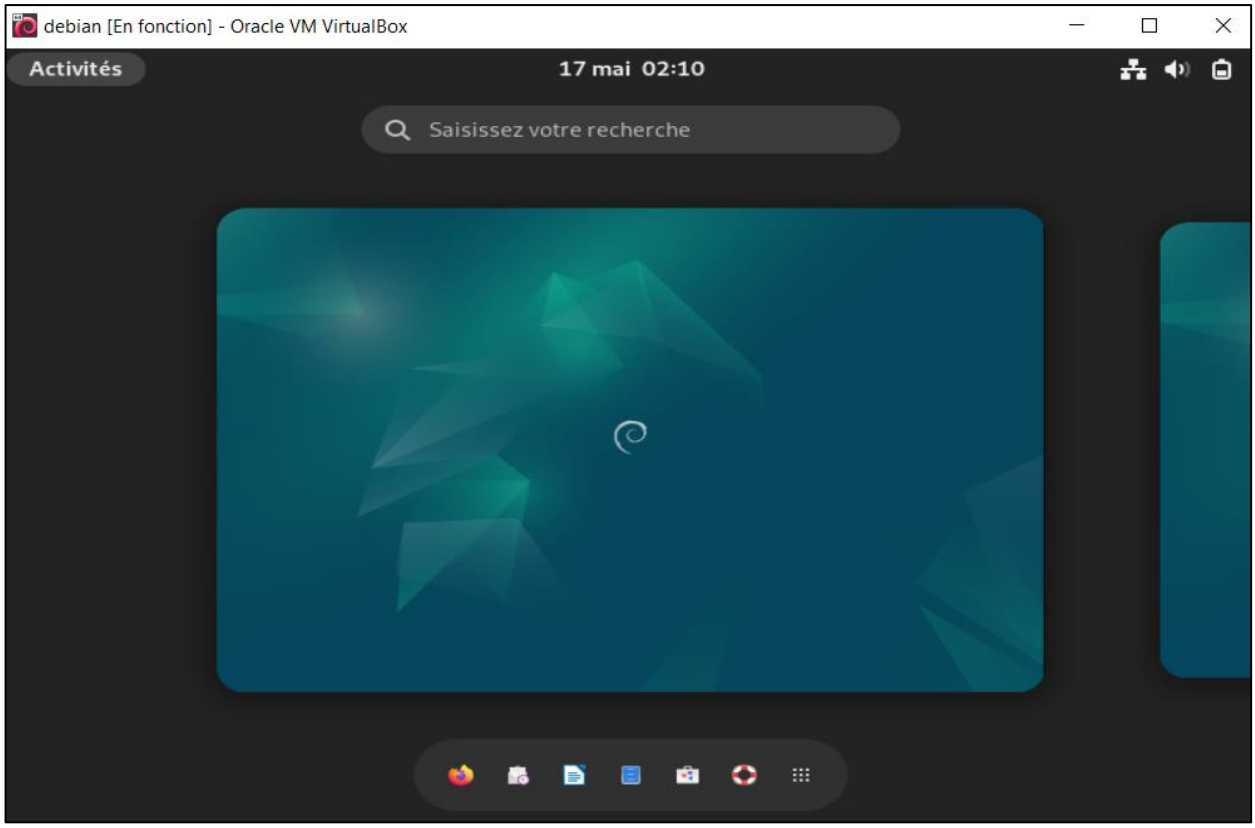
VirtualBox هو مشرف أجهزة من النوع 2. إنه مفتوح المصدر، متعدد المنصات وعالي الأداء. تم تطويره في البداية بواسطة Sun Microsystems تحت اسم Sun VirtualBox وهو الآن منتج تابع لشركة Oracle ومتوفر مجاناً كبرنامج مفتوح المصدر بموجب شروط ترخيص الرخصة العامة العامة لـ GNU (GNU GPL) الإصدار 2. وبما أنه متعدد المنصات، يمكنه العمل على أي نظام تشغيل سطح مكتب حديث سواء كان Linux أو Windows أو Mac أو Solaris.إلى جانب كونه فعالاً وقوياً ومتعدد المنصات وعالي الأداء، فإن VirtualBox مجاني أيضاً، مما يجعله منتجاً جذاباً. كما أنه مشرف الأجهزة المفتوح المصدر الوحيد من نوعه.يحتوي على العديد من المكونات، مثل مشرف الأجهزة لمنصة المضيف، وواجهة برمجة التطبيقات (API) ومجموعة تطوير البرمجيات (SDK) لإدارة الأجهزة الافتراضية الضيفة، وأداة سطر الأوامر وواجهة المستخدم الرسومية (GUI) التي يمكنها إدارة الأجهزة الافتراضية الضيفة، وبعض الميزات المدمجة مثل بروتوكول سطح المكتب البعيد (RDP) الذي يمكنه الوصول إلى الأجهزة الافتراضية الضيفة عن بعد وأدوات رسومية يمكنها إدارة الأجهزة الافتراضية الضيفة أيضاً.[16]

1.تثبيت وتكوين زابيكس:

زابيكس هو نظام للرصد يُمكن من مراقبة الخوادم والأجهزة، وتوليد التنبيهات في حالة الفشل. المبدأ يكمن في وجود جهاز يجمع المعلومات محليًا مثل حالة المعالج وحالة الذاكرة وما إلى ذلك، ثم يرسلها إلى خادم زابيكس الذي يقوم بجمع هذه المعلومات وتسجيلها في قاعدة بيانات، ثم يقوم بفرزها، وبعد ذلك ينشئ رسوم بيانية عن مدة العمل[17]

1.1إنشاء الجهاز الافتراضي الضيف DEBIAN:

في VirtualBox manager، انقر على زر "جديد" في الأعلى، وستظهر معالج يساعدك في إنشاء الجهاز الافتراضي.سيطلب المعالج بعض المعلومات بناءً على ما يقدمه المستخدم، وبعد ذلك سيتم إنشاء الجهاز الافتراضي الضيف. قم بتوفير اسم للجهاز الافتراضي؛ لقد استخدمت الاسم DEBIAN. في حقل النوع، يجب تحديد Linux. إذا كنت ترغب في أن يكون نظام تشغيل آخر هو الجهاز الافتراضي الضيف، فاختره من القائمة. في حقل الإصدار، اختر DEBIAN ثم انقر على "التالي" ثم اتبع الخطوات الأخرى كما هو مخطط لها.



الشكل 5: الصفحة الرئيسية ل Debian

2.1تثبيت خادم قاعدة البياناتMariadb

نبدأ بفتح الطرفية على Debian تثبيت خادم قاعدة بيانات MariaDB لـزابيكس يعني أنه يجب إعداد خادم قاعدة بيانات MariaDB خصيصًا للاستخدام مع زابيكس .يتضمن ذلك تثبيت وتكوين MariaDB بحيث يمكنه تخزين البيانات اللازمة لزابيكس لمراقبة وإدارة الشبكات.، هذه هي الخطوة الأولى الضرورية لاستخدامه بشكل فعال، لأنه يعتمد على قاعدة بيانات موثوقة للعمل، يثبت باستخدام الأمر التالي:

#apt install -y mariadb-server

```
root@debian:/home/melissa# apt install -y mariadb-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  galera-4 gawk libcgi-fast-perl libcgi-pm-perl libconfig-inifiles-perl libdaxctl1
  libdbd-mariadb-perl libdbi-perl libfcgi-bin libfcgi-perl libfcgi0ldbl
  libhtml-template-perl libmariadb3 libndctl6 libpmem1 libsigsegv2
  libterm-readkey-perl liburing2 mariadb-client mariadb-client-core mariadb-common
  mariadb-plugin-provider-bzip2 mariadb-plugin-provider-lz4
  mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo
  mariadb-plugin-provider-snappy mariadb-server-core mysql-common pv rsync socat
Paquets suggérés :
```

الشكل 6:تثبيت Mariadb

ثم نقوم بتسجيل الدخول إلى واجهة MySQL لإنشاء قاعدة بيانات وكلمة مرور مستخدم.

Cela permet de visualiser les informations relatives aux utilisateurs MySQL, ce qui est utile pour gérer les autorisations d'accès et les paramètres de sécurité

```
root@debian:/home/melissa# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SELECT user,authentication_string,plugin,host FROM mysql.user;
+-------------+-----------------------+-----------------------+-----------+
| User        | authentication_string | plugin                | Host      |
+-------------+-----------------------+-----------------------+-----------+
| mariadb.sys |                       | mysql_native_password | localhost |
| root        | invalid               | mysql_native_password | localhost |
| mysql       | invalid               | mysql_native_password | localhost |
+-------------+-----------------------+-----------------------+-----------+
3 rows in set (0,088 sec)

MariaDB [(none)]> ALTER USER root@localhost IDENTIFIED VIA mysql_native_password;
Query OK, 0 rows affected (0,021 sec)

MariaDB [(none)]> SET PASSWORD = PASSWORD('P@ssw0rd0@123');
Query OK, 0 rows affected (0,008 sec)
```

الشكل 7:واجهة Mariadb

3.1 أوامر تنزيل وتثبيت الحزمة الرئيسية zabbix :

في نظامDebian ، يمكنك استخدام أوامر التالية :

#wgethttps://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian9_all.deb
 # dpkg -i zabbix-release_6.4-1+debian9_all.deb

```
root@debian:/home/melissa# wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/z
abbix-release/zabbix-release_6.4-1+debian12_all.deb
--2024-05-14 13:50:08--  https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-r
elease/zabbix-release_6.4-1+debian12_all.deb
Résolution de repo.zabbix.com (repo.zabbix.com)… 178.128.6.101, 2604:a880:2:d0::2062:d0
01
Connexion à repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 3540 (3,5K) [application/octet-stream]
Sauvegarde en : « zabbix-release_6.4-1+debian12_all.deb »

zabbix-release_6.4-1+ 100%[=======================>]   3,46K  --.-KB/s    ds 0s

2024-05-14 13:50:09 (43,6 MB/s) – « zabbix-release_6.4-1+debian12_all.deb » sauvegardé
[3540/3540]
```

الشكل 8:تثبيت مستودع زابيكس

ثم نقم بتصدير قاعدة البيانات الافتراضية بواسطة Zabbix في قاعدة البيانات التي تم إنشاؤها ثم الانتقال إلى واجهة سطر الأوامر لـ MySQL لتغيير الإعدادات العامة بالاوامر التالية :

```
# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-
character-set=utf8mb4 -uzabbix_user -p zabbix_db
```

يعتمد زابيكس على ثلاثة مكونات :

- الخادمserver : مسؤول عن جمع البيانات، تحليلها، وإنشاء الرسوم البيانية، وتخزينها، وتمكين المراقبة عن بعد، وما إلى ذلك.
- الوكيلagent : يُثبّت على كل جهاز مُراد مراقبته ، ويُدعم آليات "الاستطلاع والاستدراج.
- واجهة المستخدمfront end : تسمح، من خلال واجهة الويب، بتنسيق البيانات (الرسوم البيانية)، والاطلاع على أحدث القياسات.

```
root@debian:/home/melissa# apt install -y zabbix-server-mysql zabbix-frontend-php zabbi
x-nginx-conf zabbix-sql-scripts zabbix-agent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  fping libevent-core-2.1-7 libevent-pthreads-2.1-7 libmodbus5 libodbc2 libopenipmi0
  libssh-4 nginx nginx-common php-bcmath php-fpm php-ldap php8.2-bcmath php8.2-fpm
  php8.2-ldap snmpd
Paquets suggérés :
  odbc-postgresql tdsodbc fcgiwrap nginx-doc php-pear snmptrapd zabbix-apache-conf
Les NOUVEAUX paquets suivants seront installés :
  fping libevent-core-2.1-7 libevent-pthreads-2.1-7 libmodbus5 libodbc2 libopenipmi0
  libssh-4 nginx nginx-common php-bcmath php-fpm php-ldap php8.2-bcmath php8.2-fpm
  php8.2-ldap snmpd zabbix-agent zabbix-frontend-php zabbix-nginx-conf
  zabbix-server-mysql zabbix-sql-scripts
0 mis à jour, 21 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 22,7 Mo dans les archives.
Après cette opération, 68,8 Mo d'espace disque supplémentaires seront utilisés.
```

الشكل 9: تثبيت الوكيل والخادم والواجهة المستخدم

2.تكوين الزابيكس:

تتضمن عملية تكوين الزابيكس عدة خطوات، بما في ذلك تكوين خادم وتكوين قاعدة البيانات وتكوين وكلاء على الأجهزة التي ترغب في مراقبتها، وتكوين المستجيبات والإجراءات والتنبيهات وفقًا لاحتياجاتك المحددة.

قم بتكوين ملف تكوين خادم Zabbix. بالامرالتالي:

```
# nano /etc/zabbix/zabbix_server.conf
```

ونقوم بالتعديل الملف بهذه المعلومات :

```
NomDB=zabbix_db
DBUser=utilisateur_zabbix
DBpassword=P@ssw0rd0@123
```

ثم قم بالتسجيل والخروج.

- الان نكتب عنوان IP الخاص بالخادم الخاص .

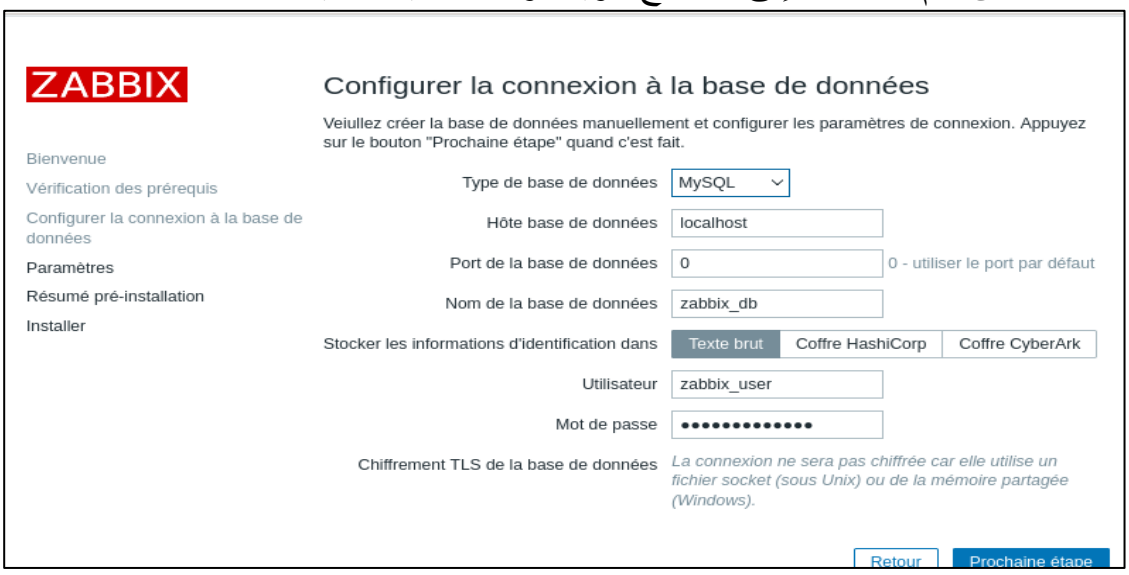
```
server {
        listen          80;
        server_name     192.168.1.41;
```

الشكل 10:عنوان IP الخاص بالخادم الخاص

- الآن أعد تشغيل الخدمة باستخدام الأمر التالي:

```
# systemctl restart zabbix-server zabbix-agent nginx php8.2-fpm
```

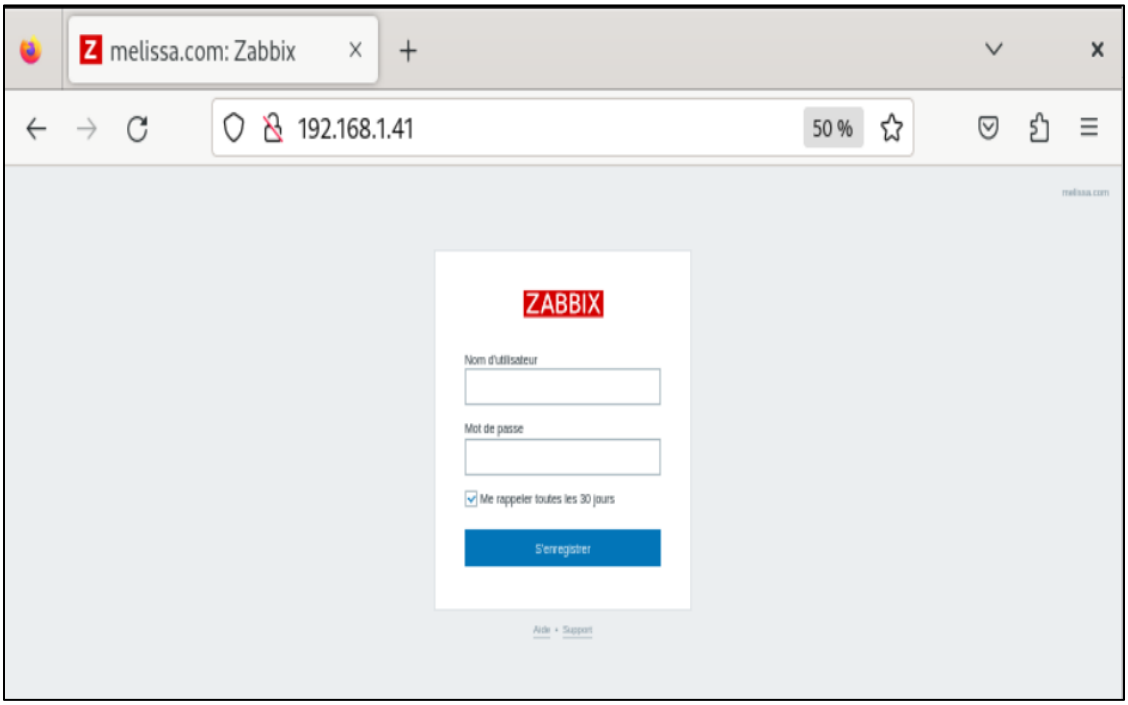
- الان نقم بالانتقال إلى متصفح الويب وبدء عملية التثبيت.



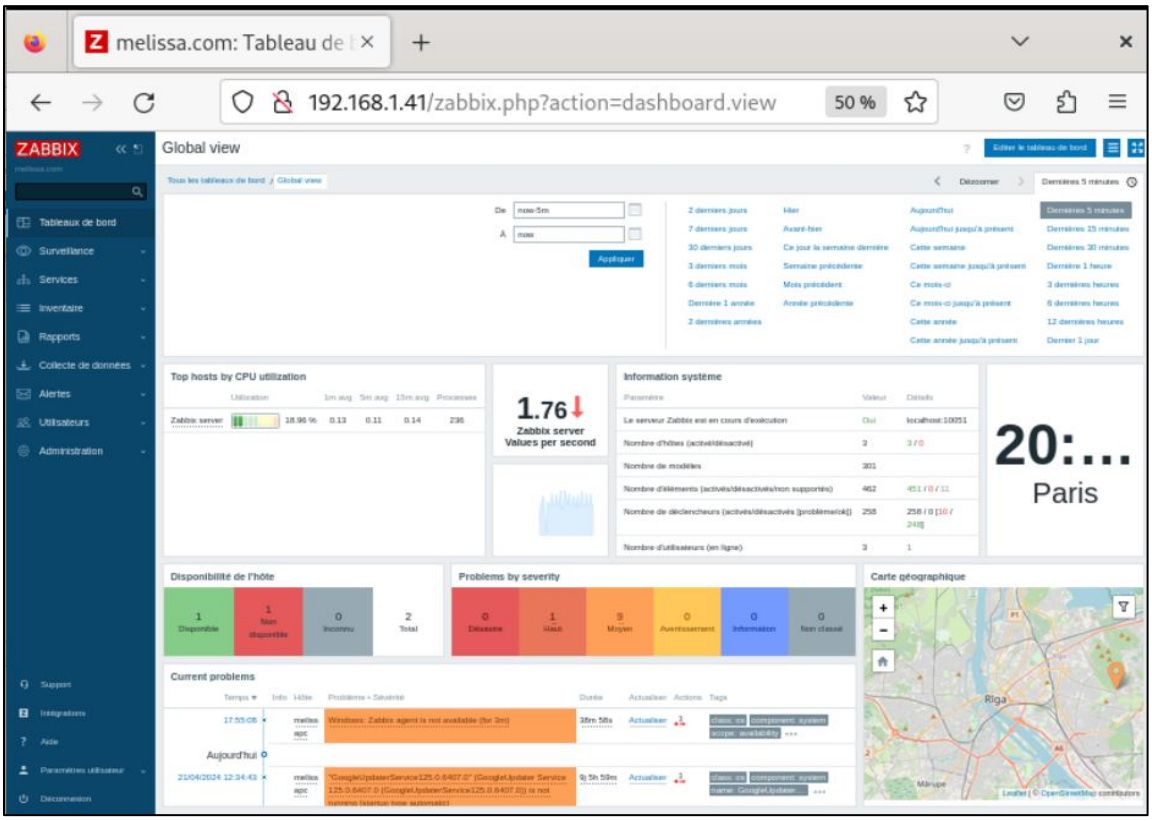
الشكل 11: تكوين اتصال قاعدة البيانات

CyberArk est idéal pour les grandes entreprises cherchant à sécuriser et gérer les accès privilégiés dans des environnements complexes

Haship Vault est mieux adapté aux environnements modernes



الشكل 12: ادخال المستخدم

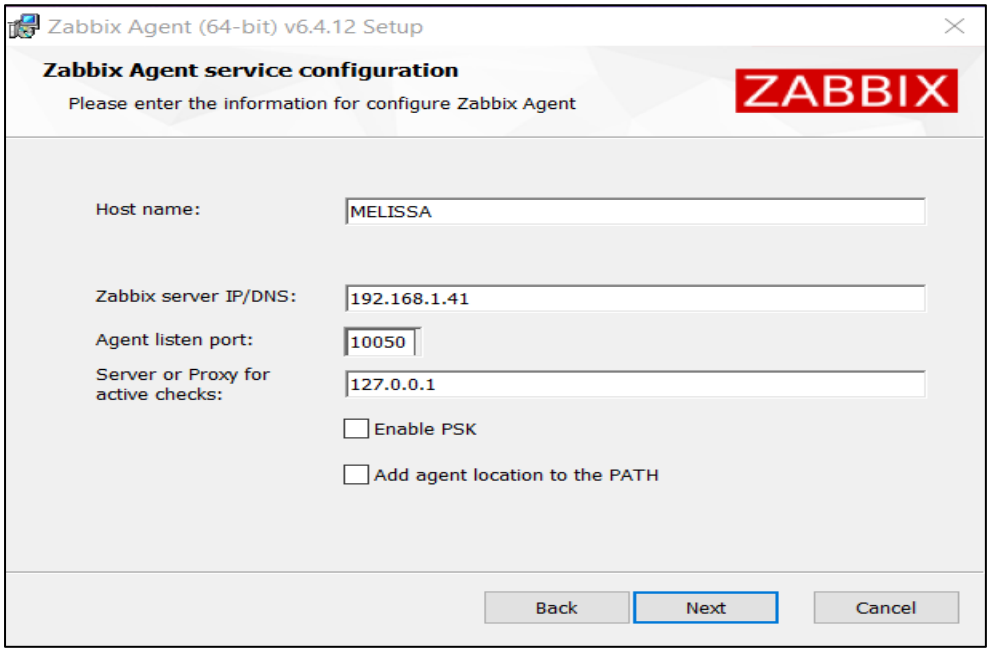


الشكل 13:متصفح الرئيسي زابيكس

3. مراقبة الشبكة على ويندوز 10:

1.3. تثبيت وكيل زابيكس على ويناوز 10 مُراد مراقبته :

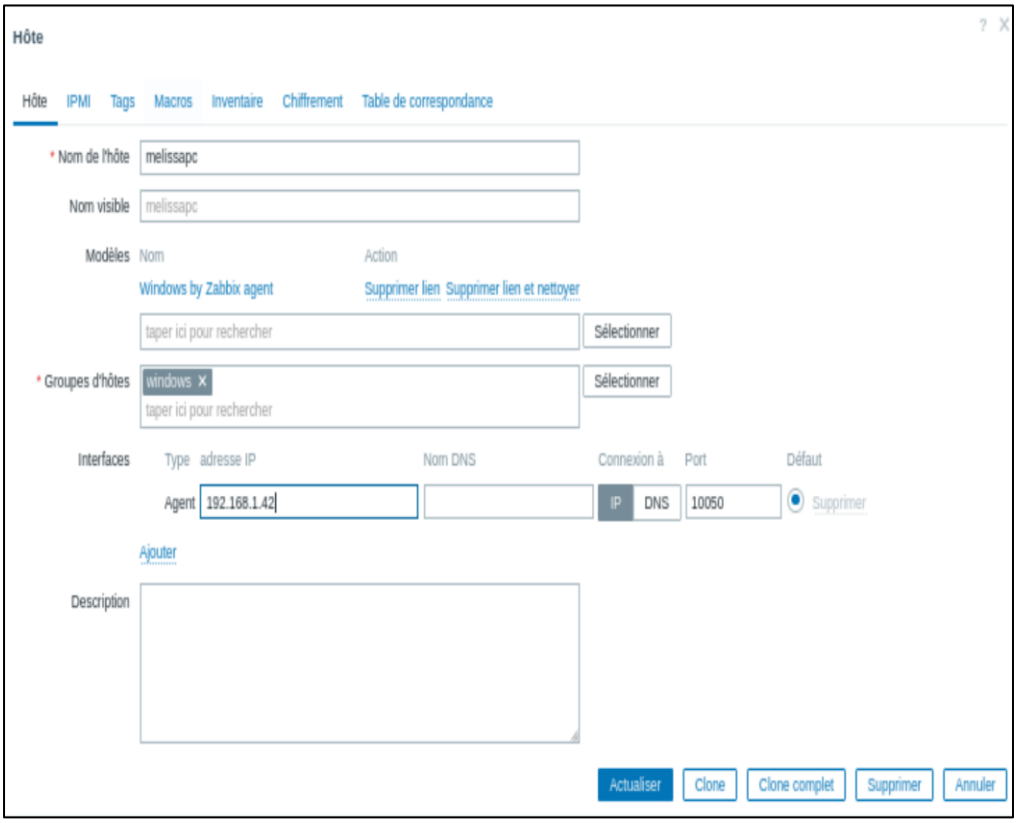
بعد تثبيت بروتوكول وكيل زابيكس من موقع زابيكس الرسمي، يمكنك الوصول إلى جهاز Windows 10 عن طريق إدخال عنوان IP لخادم زابيكس.



الشكل 14:الوكيل زابيكس

2.3 انشاء المضيف على زابيكس:

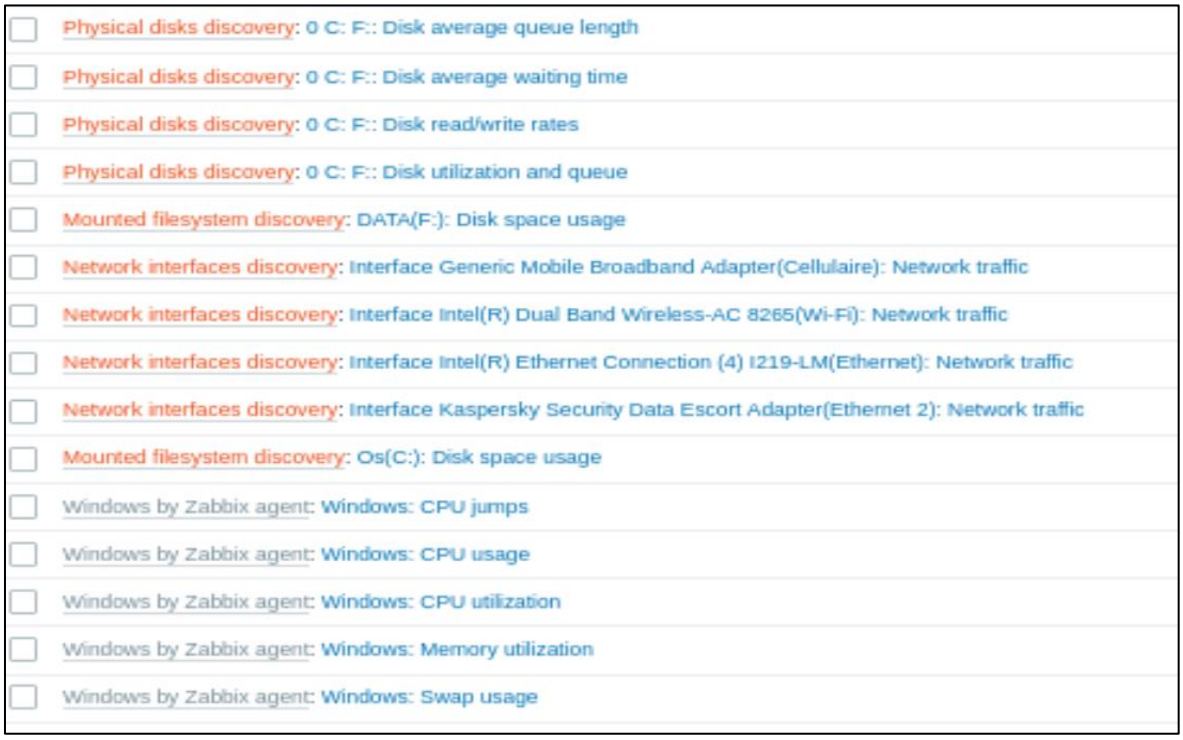
سنبدأ أولا بإنشاء مجموعة نطلق عليها اسم "windows"، ومن هناك يمكننا الانتقال إلى الأجهزة وإنشائها وإضافتها إلى المجموعة التي أنشأناها الجانب الجذاب في زابيكس هو أنه يمكننا ربط العملاء الذين لديهم وكيل زابيكس مثبتا مباشرة ثم نضيف عنوان IP للعميل بمجرد ربط الجهاز بالعميل ويندوز10 ، نطبق نموذجًا يحتوي على عناصر مثل المُشغلات والرسوم البيانية. في الواقع، هذه وظائف مُعرفة مُسبقًا لنوع معين من الأجهزة. نختار النموذج الذي يتناسب مع عميلنا من ويندوز باستخدام وكيل زابيكس .



الشكل 15: المضيف "hote"

4.تحليل بصري للأداء:

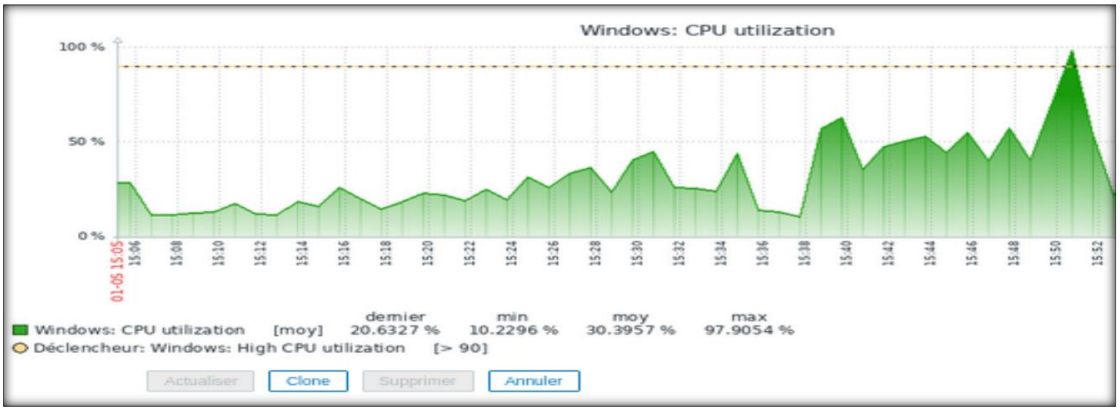
زابيكس يقدم واجهة سهلة الاستخدام لعرض بيانات الرصد، بالإضافة إلى ذلك، زابيكس يقدم مجموعة متنوعة من الرسوم البيانية والمخططات لتحليل أداء شبكتك بصورة بصرية. بالإضافة إلى مراقبة الوقت الحقيقي، زابيكس يتيح تحليل اتجاهات الأداء على فترة زمنية معينة. إليك بعض التحليل:



الشكل 16:العرض بيانات الرصد

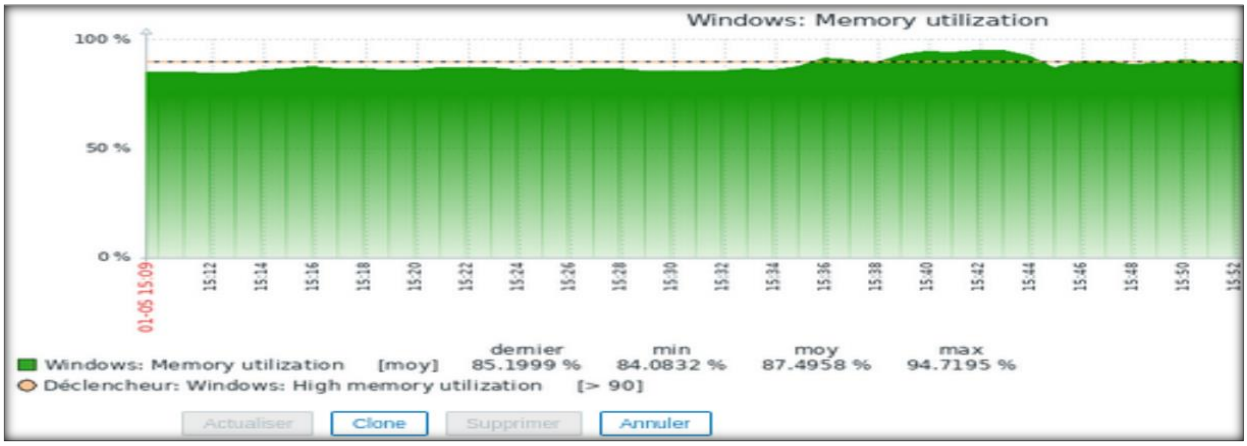
1.4بعض الرسوم البيانية :

- استخدام وحدة المعالجة المركزية (CPU) لوينداوز



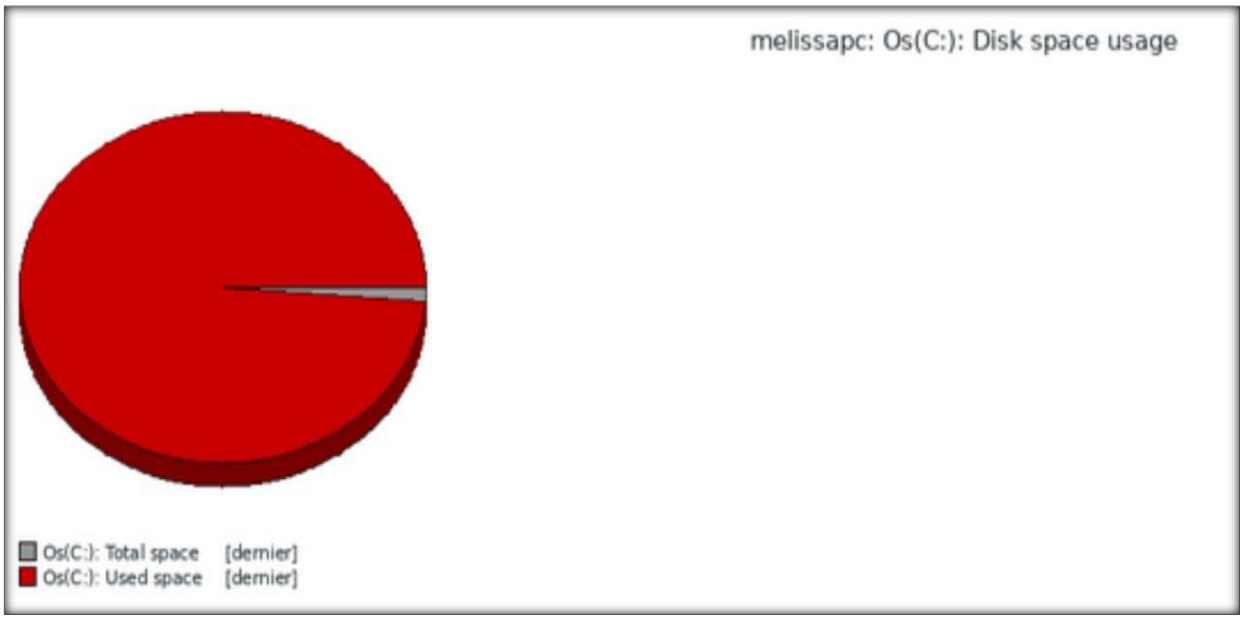
الشكل 17:رسم بياني وحدة المعالجة المركزية (CPU)

- استخدام الذاكرة لوينداز



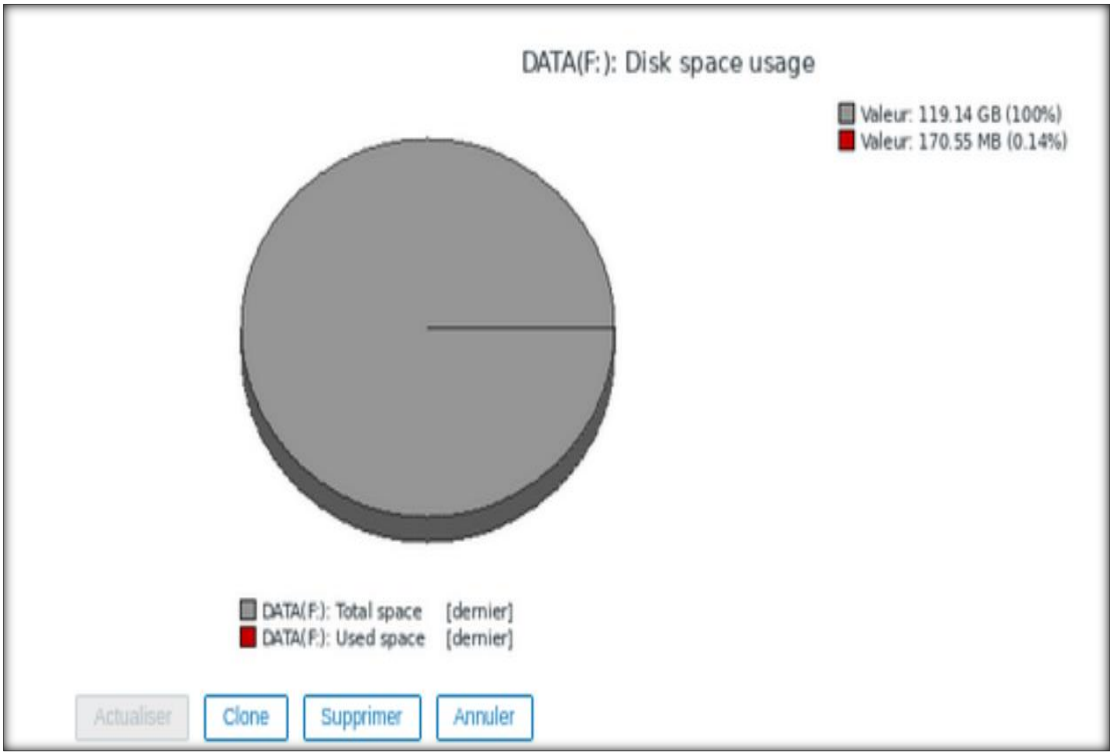
الشكل 18:رسم بياني الذاكرة لوينداز

- استخدام مساحة القرص(:c-) OS



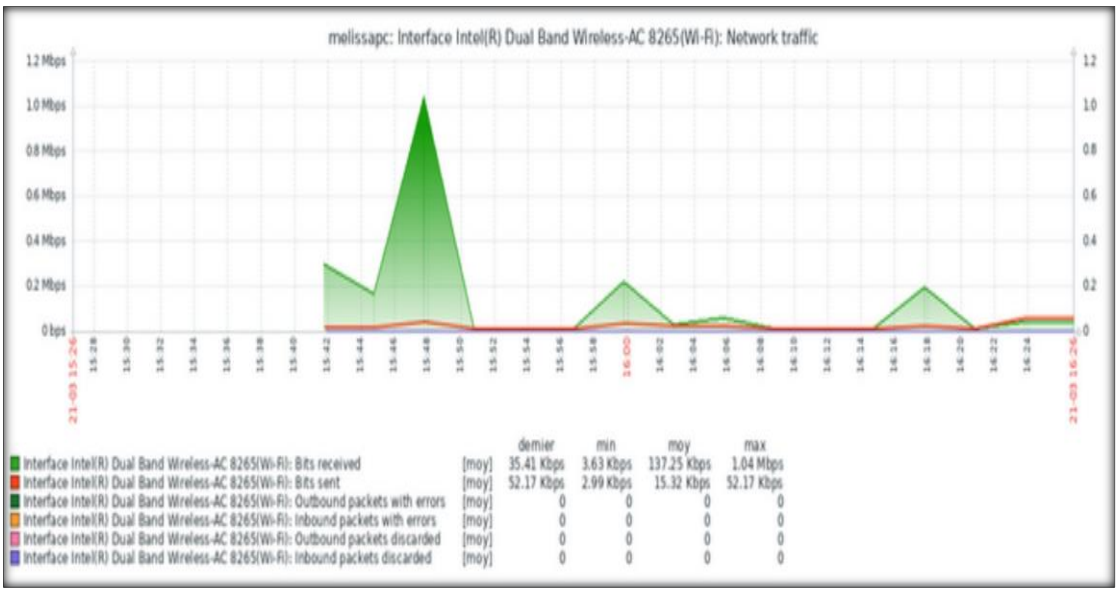
الشكل 19:دائرة بيانية مساحة القرص (:c-) OS

- استخدام مساحة القرص(:DATA(F



الشكل 20:دائرة بيانية مساحة القرص(:DATA(F

- اكتشاف واجهة الشبكة



الشكل 21:رسم بياني واجهة الشبكة

5.التنبيهات المُرسلة عن طريق زابيكس:

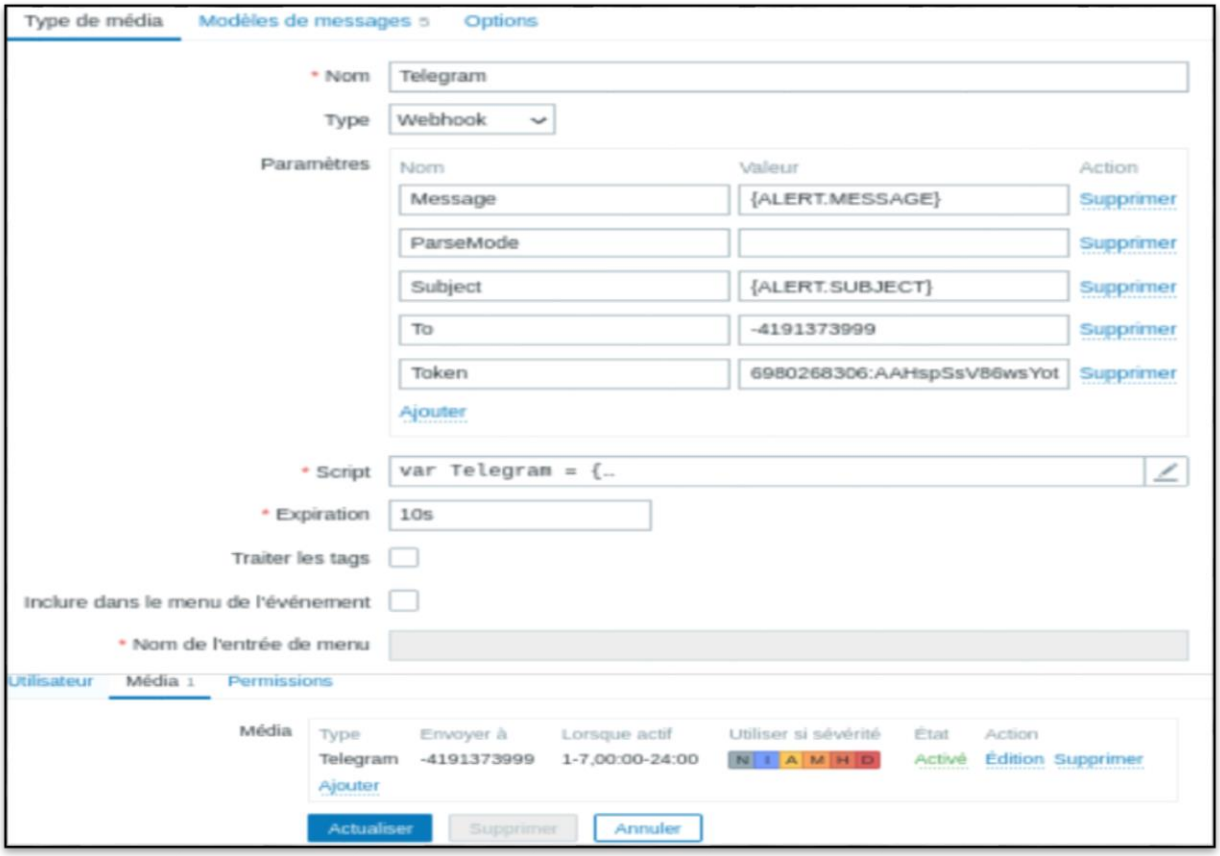
تعتبر التنبيهات التي يرسلها زابيكس إشعارات تُخطر المستخدمين عند حدوث حدث محدد في البنية التحتية التي تُراقب. يمكن أن تتم إثارة هذه التنبيهات بسبب شروط متعددة مثل فشل في الأجهزة، أو استخدام زائد للموارد، أو أي حدث آخر يُعرفه المستخدم كحرج أو يتطلب اهتمامًا فوريا. عندما يكتشف زابيكس مثل هذه الحالة، يُرسل تنبيهًا عبر القنوات المُكونة، مثل تيليجرام في حالتك. يمكن أن يحتوي هذا التنبيه على معلومات مفصلة حول الحدث، مثل اسم المضيف المعني، ووصف المشكل.

1.5 تكوين زابيكس لإرسال تنبيهات باستخدام تطبيق تليجرام:

يتم تكوين زابيكس لإرسال التنبيهات باستخدام تطبيق Telegram يتضمن عدة خطوات:

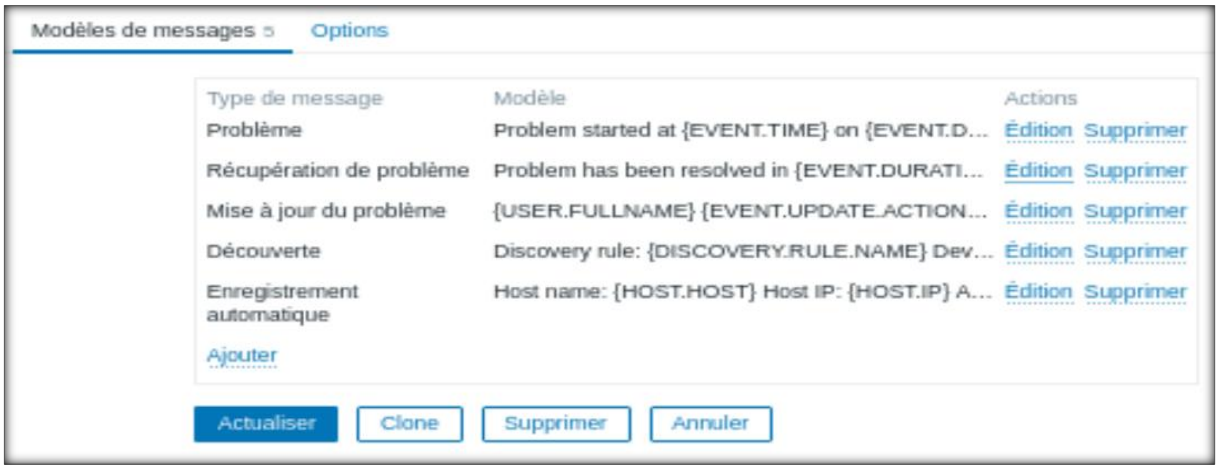
- تثبيت تطبيق Telegram على الهاتف الذكي الخاص بك.
- البحث عن "BotFather" في Telegram وابدأ الدردشة معه.
- اتباع التعليمات لإنشاء بوت جديد والحصول على توكن (Token) له

ثم نذهب إلى zabbix ونختار نوع الوسائط Telegram ثم نقوم بانشاءه و ادخال معلومات كما موضح في الشكل التالي :



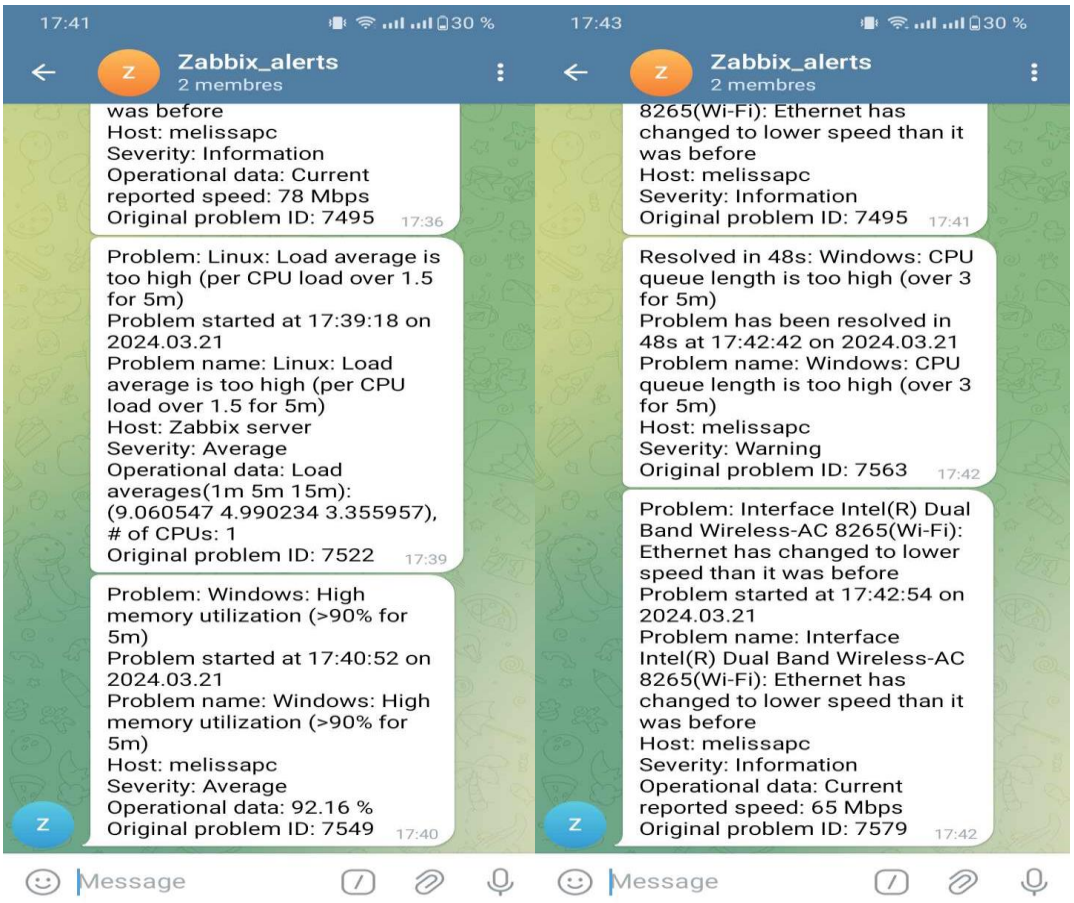
الشكل 22:تكوين تطبيق تليجرام

2.5. نموذج الرسالة



الشكل 23:صياغة الرسالة

3.5 الرسائل المستلمة



الشكل 24:الرسائل المستلمة

الخاتمة

بمجرد تثبيت زابيكس وتكوينه وبدء استقبال التنبيهات، يبدو أن زابيكس يقدم وسيلة شاملة وفعالة لرصد بنية البنية التحتية لتكنولوجيا المعلومات. بفضل ميزاته المتقدمة، مثل سهولة التكوين، وإنشاء بيانات مفصلة، والقدرة على إرسال التنبيهات في الوقت الفعلي عبر منصات مختلفة، يتيح زابيكس لمديري البنية التحتية رصد وإدارة بيئتهم التكنولوجية بنشاط. بالحصول على إشعارات دقيقة ومناسبة، يمكن للمستخدمين اتخاذ إجراءات فورية لحل المشكلات المحتملة قبل أن تتحول إلى حوادث كبيرة، مما يسهم في الحفاظ على المرونة والأداء الجيد للأنظمة. بشكل عام، زابيكس هو حلاً قويًا وموثوقًا يلعب دورًا أساسيًا في إدارة البنى التحتية لتكنولوجيا المعلومات الحديثة.

خاتمة عامة

خاتمة عامة

من خلال هذا البحث، تمت دراسة زابيكس كأداة لمراقبة وإدارة الشبكات ونظام المراقبة، حيث تم توضيح دورها في تحسين وإدارة أداء الشبكات بشكل فعال، والمساهمة في استدامة أعمال المؤسسات وتطويرها بثقة وأمان .قُدِّمَت نظرة شاملة حول عملية تثبيت وتكوين زابيكس ، مع شرح مفصل لمكوناتها ووظائفها . تم توضيح أهمية استخدام زابيكس في مراقبة الشبكات وإدارة الأخطاء والأعطال، مما يُسهِم في الحفاظ على استقرار البنية التحتية للشبكة وتحسين كفاءتها .تم تنظيم الموضوع في هيكل متين من ثلاثة فصول، لتسهيل فهم المحتوى وتقديم استنتاجات قوية وموثوقة وفي النهاية، يظهر بوضوح أن زابيكس ليس مجرد أداة لمراقبة الشبكات، بل هو شريك استراتيجي يوفر حلولًا متكاملة ومبتكرة تساهم في نجاح الشركات وتمكينها من تحقيق التميز والتفوق في عالم التكنولوجيا الحديثة.

الملخص:

في عصر الرقمنة، أصبحت الإنترنت أداة أساسية لتبادل المعلومات والتفاعل مع العالم الخارجي. توفر الوصول السريع للبيانات والخدمات وتبادل الرسائل بلا حدود. لكن وضع المعلومات الحساسة على الشبكة يتطلب أمانًا واستقرارًا ضروريين. لذا، تصبح مراقبة الشبكة أمرًا حيويًا..في هذا السياق، يأتي دور مراقبة الشبكات الذي تم التطرق اليه في هذا البحث حيث سيتناول الفصل الأول من هذه الدراسة نافذة لاستكشاف عالم مراقبة شبكات الاتصال، وسيتم التعرف على مفهوم مراقبة الشبكيات "شبكات الاتصال" واساسياتها بشكل عام كما سيتم التركيز في هذا الفصل على المواضيع الاساسية مثل اهم البروتوكولات لمراقبة الشبكة، مزايا مراقبة الشبكة، الحاجة لاستعمال برامج المراقبة ...الخ

أما في الفصل الثاني الذي جاء بعنوان " تحليل وتحسين أداء البنية التحتية للشبكات " فقد بدأنا الدراسة بتحليل متطلبات النظام والبنية التحتية المناسبة لتنصيب زابيكس تشمل الخطوات التالية نبذة مختصرة عن تاريخ زابيكس,مع ذكر اهميته و مميزاته وضع مقارنة بين بعض ادوات المراقبة...الخ.

تستند الدراسة إلى منهجية علمية دقيقة، حيث تم في الفصل الثالث توثيق كل خطوة من خطوات العمل بزابيكس بدقة مع اختبارها بارسال الرسائل عبر تطبيق telegram . يقدم البحث نتائج ملموسة تُلقي الضوء على جدوى استخدام زابيكس في بيئة معينة. نطمح في دراستنا في المستقبل الى اختباره مع باقي التطبيقات مثل الرسائل القصيرةsms و الفيسبوك وغيره مع دراسة ومراقبة حالة عمل مراكز معلوماتية أخرى مثل أجهزة الكمبيوتر، المحولات، الجدران النارية وحتى البرامج .

Résumé :

En cette ère de numérisation, Internet est crucial pour échanger des informations, nécessitant une sécurité et une stabilité accrues pour les données sensibles. Cette recherche souligne l'importance de la surveillance des réseaux, explore les fondamentaux et les protocoles de surveillance, et analyse l'installation et les avantages de Zabbix en comparaison avec d'autres outils. Elle documente également l'utilisation de Zabbix avec des tests d'envoi de messages via Telegram, avec des perspectives de tests futurs incluant d'autres applications et centres informatiques.

المصادر و المراجـع

[1] https://robodin.com/network-monitoring/ ,consulté le 23/03/2024 .

[2] https://www.it-pillars.com,consulté le 23/03/2024 .

[3] https:// - Dotcom-Monitor Web Performance Blog,consulté le 23/03/2024 .

[4] http://www.almarefa.blogspot.com/2010/02/blog-post. ,consultéle 24/03/2024 .

[5] https://www.monitoring-fr.org/supervision/html,consulté le 24/03/2024 .

[6] https://academy.hsoub.com/devops/networking/,consulté le 24/03/2024 .

[7] https://www.solarwinds.com/netflow-traffic-analyzer ,consulté le 24/03/2024 .

[8] https://arab-ency.com.sy/,consulté le 26/03/2024

[9] https://www.dotcom-monitor.com,consulté le 28/03/2024

[10]http://conectclub.blogspot.com/zabbix.html,consulté le 28/03/2024 .

[11]https://www.monitoring-network.com,consulté le 20/04/2024 .

[12]https://www.fobramg.com/2021/10/best-network-monitoring-tools.html,consulté le 20/04/2024

[13]Sukhija N, Bautista E, James O, Gens D, Deng S, Lam Y, Quan T and Lalli B. Event Management and Monitoring Framework for HPC Environments using ServiceNow and Prometheus. Proceedings of the 12th International Conference on Management of Digital EcoSystems. November 2020 (149-156).

[14]https://www.dotcom-monitor.com/blog/ar/,consulté le 21/04/2024 .

[15]Andrea Dalle Vacche, Stefano Kewan Lee , Zabbix Network Monitoring Essentials,Your one-stop solution to efficient network monitoring with Zabbix (2015, Packt Publishing)

[16]Dash, Pradyumna. Getting Started with Oracle VM VirtualBox. First ed., Packt Publishing Ltd., December 2013.

[17]www.zabbix.com,consulté le 21/04/2024

[18]https://ram-0000.developpez.com/tutoriels//SNMP/,consulté le 21/04/2024

[19]https://robodin.com/network-monitoring/,consulté le 22/04/2024

[20]Network Administration and Monitoring Tools - Example NAGIOS ,Thierry Briche and Matthieu Voland ,Report , December 2004"

الاختصارات

1. SNMP (Simple Network Management Protocol)
2. RMON (Remote Network MONitoring)
3. CMIP(Common :Management Information Protocol)
4. CMIS (Common Management Information Services)
5. CMISE (Common Management Information Service Element)
6. MIB (Management Information Bases)
7. DoS(Disk Operating System)
8. TCP/IP (Transmission Control Protocol/Internet Protocol)
9. CMOT (CMIP Over TCP)
10. LAN(Local Area Network)