الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA 1

كلية التكنولوجيا
Faculté de Technologie

قسم إلكترونيك
Département d'Électronique

MEMOIRE DE MASTER

Filière : Télécommunication
Spécialité : Réseaux et Télécommunications

Présenté par :

- **BENTEBICHE Ibtissem**
- **DOUA Rafah**

Supervision des plateformes de TOIP pour les sociétés du groupe Sonelgaz

Proposé par :

Promoteur : Mr HOUA Zakaria

Co-promoteur : Mr BENDOUMIA Redha

Année Universitaire : 2023-2024

Remerciement

Ce jour marque la fin d'une longue période d'étude à l'université de SAAD DAHLAB de BLIDA. Au terme de notre formation en générale et notre projet de fin d'étude en Particulier.

Nous tenons tout d'abord à remercier Allah le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce Modeste travail.

En second lieux, Nous tenons à exprimer nos profondes gratitudes à tous ceux qui ont contribué à la réalisation de ce mémoire sur la " Supervision des plateformes de TOIP pour les sociétés du groupe Sonelgaz" . Ce projet n'aurait pas pu aboutir sans le soutien et l'implication de nombreuses personnes.

Nos remerciements notre promoteur M. HAOUA Zakaria qui fut proposer ce sujet est nous a guidées et conseillées tout au long de cette recherche. Son expertise et son dévouement ont été les piliers pour le développement de ce travail.

Un sincère merci aux Notre Co-promoteur M. BENDOUMIA Redha qui est généreusement partagé leur expertise lors des entretiens et des échanges d'idées. Leurs contributions ont grandement enrichi la portée de ce mémoire.

Enfin, nous tenons à remercier l'équipe pédagogique et le personnel de Elit Sonelgaz pour les ressources mises à disposition et l'environnement propice à l'apprentissage et à la recherche.

ملخص

لقد بدأ ToIP ثورة في الاتصالات التجارية من خلال تقديم بديل مالي للأنظمة الهاتفية التقليدية. استخدمت Sonelgaz هذه التكنولوجيا لتعزيز الاتصالات الداخلية وتقليل التكاليف. يهدف هذا المشروع إلى ضمان توفر وتأمين البنية التحتية ToIP من خلال إنشاء نظام مراقبة مفتوح المصدر، Nagios، لتنظيم شبكة هاتفية تستند على FreePBX وIssabel.
وتشمل الأهداف اكتشاف الأخطاء في وقت مبكر وتحديث المشكلات بسرعة لضمان استمرار الخدمات. عملت حلولنا بشكل فعال، حيث تم اكتشاف المشكلات بسرعة وإبلاغ المسؤولين المعنيين. هذا تمكن من التدخل الإبداعي، مما أدى إلى تقليل وقت الإزعاج وتأمين الاتصال السلبي داخل Sonelgaz.

كلمات المفاتيح: ToIP, Sonelgaz , supervision, Nagios

Résumé

La ToIP a révolutionné les communications d'entreprise en offrant une alternative économique aux systèmes téléphoniques traditionnels. Sonelgaz a intégré cette technologie pour améliorer la communication interne et réduire les coûts. Ce projet vise à garantir la disponibilité et la fiabilité des infrastructures ToIP en mettant en place un système de supervision open-source, Nagios, pour superviser un réseau téléphonique basé sur FreePBX et Issabel. Les objectifs incluent la détection précoce des anomalies et la résolution rapide des problèmes pour assurer la continuité des services. Notre solution fonctionnait efficacement, les problèmes étant rapidement détectés et notifiés aux responsables concernés. Cela a permis une intervention proactive, minimisant ainsi les temps d'interruption et assurant une communication fluide au sein de Sonelgaz.

Mots clés : ToIP, Sonelgaz, supervision, Nagios.

Abstract

ToIP has revolutionized corporate communications by offering a cost-effective alternative to traditional telephone systems. Sonelgaz has integrated this technology to improve internal communication and reduce costs. The project aims to ensure the availability and reliability of ToIP infrastructures by implementing an open-source surveillance system, Nagios, to oversee a telephone network based on FreePBX and Issabel. Objectives include early detection of anomalies and rapid troubleshooting to ensure service continuity. Our solution worked effectively, with problems quickly detected and notified to the responsible persons concerned. This enabled proactive intervention, thus minimizing interruption times and ensuring smooth communication within Sonelgaz.

Keywords : ToIP, Sonelgaz, supervision, Nagios

TABLE DES MATIERS

Chapitre I : Présentation de l'organisme d'accueil

Chapitre II : Généralité sur la VOIP

Chapitre III : Choix de la solution de supervision

Chapitre IV : Réalisation et Test

LISTE DES ACRONYMES ET ABREVIATIONS

ARCPE : **A**utorité de **R**égulation des **T**élécoms

ACD : **A**dvanced **C**all **D**istribution

CDR : **C**all **D**etail **R**ecords

DAHDI : **D**igium **A**sterisk **H**ardware **D**evice **I**nterface

EGA : **E**lectricité et **G**az d'**A**lgérie

ELIT : **EL** Djazair **I**nformation **T**echnology

GSM : **G**lobal **S**ystem for **M**obile Communication

GPL : **G**eneral **P**ublic **L**icense

IP : **I**nternet **P**rotocol

IAX : **I**nter-**A**sterisk e**X**change

ITU : **I**nternational **T**élécommunications **U**nion

ISDN : **I**ntegrated **S**ervice **D**ata **N**etwork

IETF : **I**nternet **E**ngineering **T**ask **F**orce

IVR : **I**nteractive **V**oice **R**esponse

LAN : **L**ocal **A**rea **N**etwork

MCU : **M**ultipoint **C**ontrol **U**nit

MGCP : **M**edia **G**ateway **C**ontrol **P**rotocol

MRTG : **M**ulti **R**outer **T**raffic **G**rapher

NAT : **N**etwork **A**ddress **T**ranslation

PSTN : **P**ublic **S**witched **T**elephone **N**etwork

PABX : **P**rivate **A**utomatic **B**ranch E**X**change

QOS : **Q**uality **O**f **S**ervice

RTC : **R**éseau **T**éléphonique **C**ommuté

RNIS : **R**éseau **N**umérique à **I**ntégration de **S**ervices

RTSP : **R**eal **T**ime **S**treaming **P**rotocol

RSVP : **R**esource Re**S**er**V**ation Protocol

RTCP : **R**eal-time **T**ransport **C**ontrol **P**rotocol

RAS : **R**egistration/**A**dmission/**S**tatus

SIP : **S**ession **I**nitiation **P**rotocol

SDP : **S**ession **D**escription **P**rotocol

LISTE DES ACRONYMES ET ABREVIATIONS

SNMP : **S**imple **N**etwork **M**anagement **P**rotocol

TCP : **T**ransmission **C**ontrol **P**rotocol

ToIP : **T**elephony **o**ver **I**nternet **P**rotocol

UDP : **U**ser **D**atagram **P**rotocol

VoIP : **V**oice **o**ver **I**nternet **P**rotocol

WAN : **W**ide **A**rea **N**etwork

WLAN : **W**ireless **L**ocal **A**rea **N**etwork

WWAN : **W**ireless **W**ide **A**rea **N**etwork

INTRODUCTION GÉNÉRALE

La VoIP (Voice over Internet Protocol) a radicalement transformé la manière dont les entreprises communiquent, offrant une alternative efficace et économique aux systèmes de téléphonie traditionnels. Son intégration au sein du groupe SONELGAZ a été un élément clé dans l'amélioration de la communication entre les différentes entités, la promotion de la flexibilité opérationnelle et la réduction des coûts. Cependant, la fiabilité de ces systèmes est cruciale, car toute défaillance pourrait avoir des conséquences désastreuses, impactant non seulement la productivité interne, mais aussi la capacité à répondre aux besoins des citoyens.

Dans ce contexte, ce projet de fin d'étude se propose d'adresser une problématique essentielle.

Problématique : comment garantir la disponibilité et la fiabilité des infrastructures VoIP au sein du groupe SONELGAZ, tout en assurant une réactivité optimale face aux incidents ?

Objectif : Pour répondre à cette question, l'objectif principal de ce projet est de mettre en place un système de supervision basé sur une solution open source, permettant de surveiller en temp réel l'état de l'ensemble des infrastructures téléphoniques déployées à travers le territoire national. Cette supervision vise à détecter précocement les anomalies, à résoudre rapidement les problèmes potentiels et à garantir la continuité des services, le tout en intégrant un système d'alerte efficace pour informer les responsables et les techniciens dès l'apparition d'une défaillance.

Plusieurs tâches sont identifiées. Tout d'abord, il s'agira de mettre en place un serveur de supervision sur un environnement de simulation, puis sur un serveur réel. Ensuite, des scripts et des templates seront développés pour chaque marque de serveur téléphonique afin de collecter et de transmettre les informations sur l'état des services téléphoniques au serveur de supervision. Parallèlement, une interface web intuitive sera conçue pour permettre aux utilisateurs autorisés de visualiser en temps réel l'état des serveurs téléphoniques et de leurs services, tout en conservant un historique des états passés. Cette interface intégrera également un système de classification des incidents selon leur gravité, facilitant ainsi la prise de décision et l'assignation des priorités d'intervention.

Enfin, cette solution inclura un mécanisme automatisé d'envoi de notifications par e- mail aux personnes concernées en cas de défaillance sur l'un des serveurs, garantissant ainsi une réactivité optimale face aux incidents. De plus, un rapport mensuel résumant le temps de disponibilité de l'infrastructure VoIP sera automatiquement généré et envoyé au responsable

désigné, offrant ainsi une visibilité accrue sur la performance du système et permettant d'identifier d'éventuelles tendances ou problèmes récurrents.

Ce travail réalisé est subdivisé sur quatre chapitres :

Chapitre 1 : Présentation de l'organisme d'accueil

Dans le Chapitre, nous allons présenter l'entreprise SONELGAZ, en détaillant ses départements et en recueillant des informations pertinentes pour notre travail.

Chapitre 2 : Généralité sur la VoIP

Dans ce chapitre, nous allons exposer une introduction détaillée sur les principes et le fonctionnement de la VoIP. Nous explorerons ses avantages, ses limitations et ses applications, fournissant ainsi les bases nécessaires pour comprendre les défis et les opportunités de sa mise en œuvre au sein du groupe SONELGAZ.

Chapitre 3 : Etude de l'existence et du choix de la solution de supervision

Dans ce chapitre, l'accent sera mis sur le processus de sélection d'une solution de supervision adaptée aux besoins du groupe SONELGAZ. L'étude analysera les différentes options disponibles, évaluant leurs fonctionnalités, leurs coûts et leur compatibilité avec l'infrastructure existante afin de justifier le choix final de la solution de supervision.

Chapitre 4 : Réalisation et tests

Le dernier chapitre décrit la mise en œuvre du système de supervision retenu et les tests réalisés pour évaluer sa performance. Il détaille les étapes de déploiement, la création de scripts et Template, ainsi que le développement de l'interface utilisateur. Les résultats des tests sont analysés pour vérifier la conformité du système aux besoins du groupe Sonelgaz.

Chapitre I
Présentation de l'organisme d'accueil

I.1. Introduction

L'exploration de l'entité d'accueil revêt une importance capitale pour appréhender les contingences qui façonneront notre projet. SONELGAZ, opérateur historique de l'énergie en Algérie depuis sa création en 1969, a évolué d'une entreprise intégrée à une holding pilotant un groupe industriel diversifié. Dans ce premier Chapitre, nous nous attarderons sur l'entreprise SONELGAZ, en détaillant ses départements et en recueillant des informations pertinentes pour notre travail.

I.2. Présentation générale de l'organisme d'accueil

SONELGAZ joue un rôle important dans le développement économique et social du pays, elle a significativement contribué à la mise en œuvre de la politique énergétique nationale, avec des réalisations majeures telles que l'électrification rurale et la distribution de gaz. Avec une couverture électrique de 99% pour plus de 11 millions de clients et une pénétration du gaz à 65% pour plus de 7 millions de clients. SONELGAZ est composée de 11 filiales et 10 sociétés en participation, exerce ses missions de production, transport, distribution d'électricité et de gaz, tout en explorant de nouveaux segments commerciaux, notamment à l'international [1].

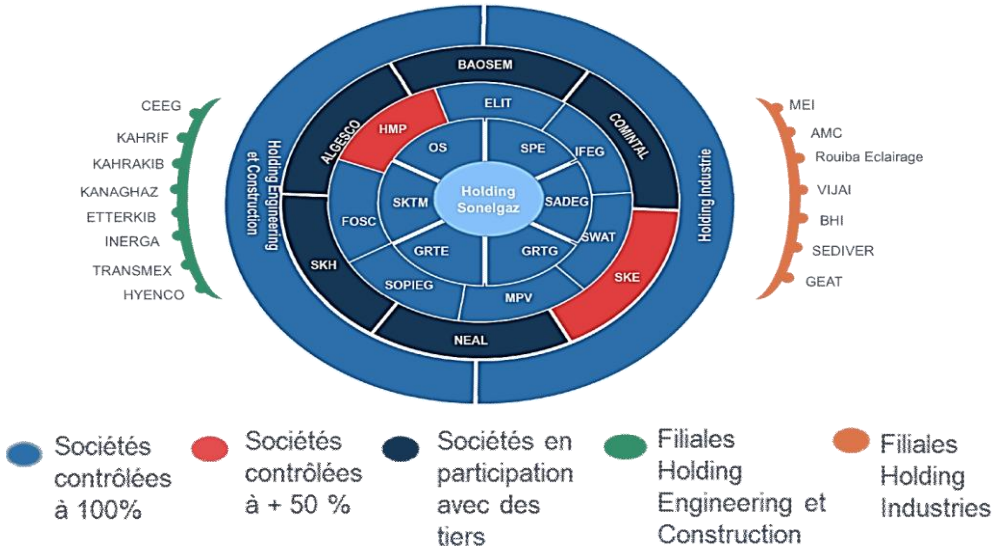


Figure I.1. L'organigramme du groupe SONELGAZ [2].

I.3. Historique

Depuis l'ère de l'EGA (Electricité et Gaz d'Algérie), qui fut le fournisseur pionnier en électricité et en gaz, jusqu'à l'émergence de Sonelgaz (Société Algérienne de l'Electricité et du Gaz) en tant que figure majeure dans le secteur énergétique national, cinquante années se sont

écoulées, marquées par un remarquable engagement dans le développement économique et social de l'Algérie, avec une influence s'étendant jusqu'au continent africain et à la région méditerranéenne [2].

I.3.1. Création de « Electricité et Gaz d'Algérie » (EGA)

En 1947, la création de « Electricité et Gaz d'Algérie » (EGA) marqua une étape décisive dans l'histoire énergétique du pays. Auparavant, le secteur de l'électricité était dominé par des concessions détenues par des entreprises coloniales, avec 16 sociétés réparties à travers l'Algérie parmi elle :

Le Groupe Lebon « Compagnie Centrale d'Eclairage par le Gaz ».

La Société Algérienne d'Eclairage et de Force « SAEF » au centre et à l'ouest.

La Compagnie du Bourbonnais à l'est.

Les usines Lévy à Constantine.

Ces concessions étaient principalement utilisées pour les besoins agricoles, l'éclairage, les usages domestiques et quelques industries. Cependant, le 8 avril 1946, l'adoption d'une loi en France métropolitaine conduisit à la nationalisation des activités électriques et gazières, une mesure qui fut également étendue à l'Algérie. Cette nationalisation a conduit à la création d'EGA le 5 juin 1947, conférant à cette nouvelle entité le monopole de la production, du transport et de la distribution d'électricité et de gaz sur l'ensemble du territoire algérien. En conséquence, les 16 sociétés concessionnaires existantes furent transférées à EGA, marquant ainsi le début d'une ère nouvelle dans le secteur énergétique du pays.

I.3.2. EGA est pris en charge par l'état Algérien indépendant en 1962

EGA est pris en charge par l'état algérien nouvellement indépendant, en quelques années grâce à un effort de formation et d'encadrement et un personnel algérien assurent effectivement le fonctionnement de l'établissement.

I.3.3. Dissolution l'EGA et création de SONELGAZ

Le grand défi … Soutenir le développement économique et social

En 1969, l'Algérie a entrepris un changement significatif dans son secteur énergétique avec la dissolution d'EGA (Electricité et Gaz d'Algérie) et la création de SONELGAZ (Société Nationale de l'Electricité et du Gaz), par ordonnance N°69-59 du 28 juillet 1969.

Ce pas marquait une rupture décisive avec l'héritage colonial, répondant ainsi aux nouvelles orientations politiques et économiques du pays.

La transformation de l'EGA en SONELGAZ visait à renforcer les capacités organisationnelles et managériales de l'entreprise pour soutenir le développement économique de l'Algérie. SONELGAZ a ainsi obtenu le monopole de la production, du transport, de la distribution, de l'importation et de l'exportation de l'électricité, ainsi que la responsabilité de l'installation et de l'entretien des appareils électriques et gaziers domestiques. De plus, elle a été chargée de promouvoir l'utilisation du gaz naturel et de l'électricité dans divers secteurs industriels, artisanaux et domestiques. Elle a également été désignée comme le seul organisme autorisé à commercialiser le gaz naturel à l'intérieur du pays pour tous les types de clients, y compris les industries et les centrales électriques. Ces changements ont propulsé SONELGAZ vers une nouvelle ère, la préparant à devenir un acteur majeur de l'industrie à l'échelle nationale et internationale au cours de ses 50 premières années.

I.3.4. Plan national d'électrification

1976 : Adoption de la charte nationale sur « la généralisation de l'électrification domestique à travers tout le territoire, avec comme objectif, d'introduire l'électricité dans la totalité des foyers algériens avant la fin de la prochaine décennie (1990) ».

A partir de 1977 : SONELGAZ s'est concentrée sur le programme d'électrification totale du pays, ce qui aura une implication majeure sur le développement des réseaux de distribution. Ainsi, elle a largement contribué à la modernisation de l'économie et à l'amélioration des conditions de vie des citoyens en Algérie.

I.3.5. Le tournant de la première restructuration

En 1983, après 14 ans d'existence, SONELGAZ entreprend sa première restructuration, donnant naissance à cinq filiales spécialisées et à une entité de fabrication. Ces filiales, relevant des Sociétés de Gestion de Participations de l'État (SGP), comprennent KAHRIF pour l'électrification rurale, KAHRAKIB pour les infrastructures électriques, KANAGHAZ pour les réseaux gaziers, INERGA pour le génie civil, ETTERKIB pour le montage industriel, et enfin AMC pour la fabrication des compteurs et appareils de mesure et de contrôle.

La réorganisation de SONELGAZ a permis de mettre en place des infrastructures électriques et gazières adaptées aux besoins socio-économiques du pays. Le modèle de "Maison-

mère et Filiales" adopté a apporté à SONELGAZ de nouvelles capacités opérationnelles et de gestion, tandis que ses filiales sont devenues des acteurs essentiels dans la réalisation des projets d'infrastructures. Cette approche a façonné le fonctionnement actuel de SONELGAZ, caractérisé par son autonomie décisionnelle et sa capacité d'adaptation rapide dans un environnement en perpétuelle évolution.

I.3.6. Un nouveau statut de SONELGAZ

Le 14 décembre 1991 : SONELGAZ change de nature juridique par décret exécutif n°91-475, Portant transformation de la nature juridique de la société nationale d'électricité et du gaz en « Etablissement Public à Caractère Industriel et Commercial » (EPIC).

La reprise de statut confirme la mission de service public et pose la nécessité de la gestion économique et de la prise en compte de la commercialité.

I.3.7. SONELGAZ devient EPIC

Le décret exécutif N° 95-280 du 17 septembre 1995 marque un tournant dans l'histoire de SONELGAZ, la transformant en un Établissement Public à caractère Industriel et Commercial (EPIC). Désormais placée sous la tutelle du Ministère en charge de l'Energie et des Mines, SONELGAZ bénéficie de la personnalité morale ainsi que de l'autonomie financière. Soumise aux règles de droit public dans ses relations avec l'État, elle est considérée comme une entité commerciale vis-à-vis des tiers. Par ce même décret, SONELGAZ se voit confier la mission essentielle de service public, renforçant ainsi son rôle crucial dans le secteur énergétique.

I.3.8. Début de la filialisation progressive de SONELGAZ

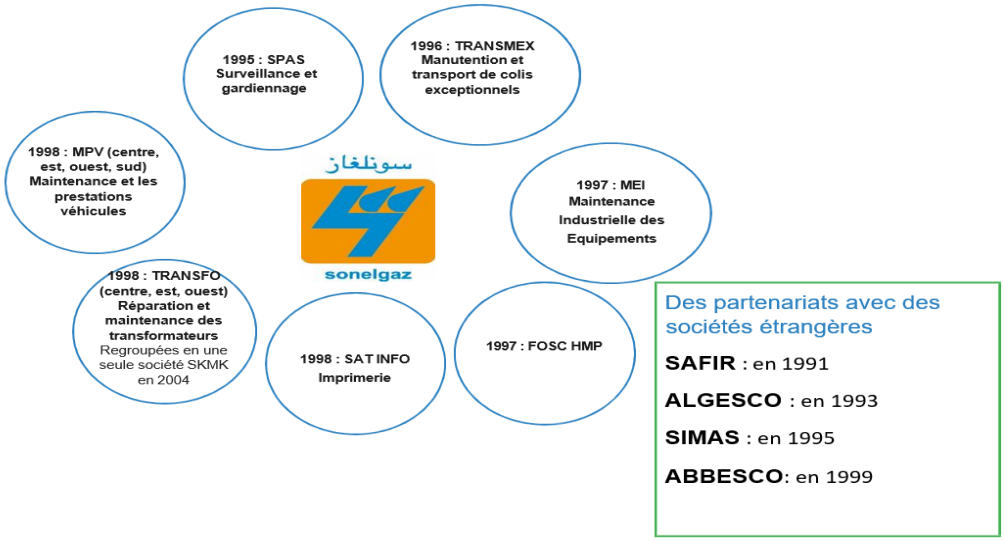


Figure I.2. Début de la filialisation progressive de SONELGAZ [2].

I.3.9. SONELGAZ devient SPA

Par le biais du Décret présidentiel n° 02-195 du 01 Juin 2002, SONELGAZ évolue vers la dénomination de Société Algérienne de l'Electricité et du Gaz, adoptant ainsi le statut de Société par Actions (SPA). Sous ce régime, elle est soumise aux réglementations de la loi sur l'électricité et la distribution du gaz par canalisations, ainsi qu'aux dispositions du code de commerce. Ce changement de statut lui ouvre de nouvelles perspectives, lui permettant d'étendre ses activités à d'autres secteurs énergétiques et même d'intervenir sur la scène internationale.

I.3.10. La naissance du Groupe Industriel SONELGAZ

En 2004, SONELGAZ franchit une nouvelle étape en devenant un Groupe Industriel avec 38 filiales. Elle se positionne en tant que leader parmi les investisseurs nationaux, jouant un rôle Crucial dans le développement économique du pays. Son objectif principal est de devenir un catalyseur pour les investissements nationaux et étrangers dans le secteur de l'énergie.

Pour atteindre cet objectif, SONELGAZ restructure son organisation en transformant ses entités chargées des activités de base en filiales distinctes, telles que la production d'électricité avec la création de la SPE, le transport de l'électricité avec la GRTE, et le transport du gaz naturel avec la GRTG. En 2004, SONELGAZ affichait un taux d'électrification dépassant 96 % et un taux de pénétration de 34 % pour le gaz naturel [2].

- En 2006 Création de (4) Sociétés de Distribution :
  - SONELGAZ Distribution Alger (SDA).
  - SONELGAZ Distribution Centre (SDC).
  - SONELGAZ Distribution Est (SDE).
  - SONELGAZ Distribution Ouest (SDO).

Réintégration des cinq (5) sociétés de travaux :

- KAHRIF.
- KAHRAKIB.
- ETTERKIB.
- KANAGHAZ.
- INERGA

- En 2007

- Création de l'Institut de formation en électricité et Gaz (IFEG).

- Réorganisation de SPE en quatre Pôles Nationaux de Production d'Electricité dont un Pôle Sud.

➢ En 2009

- Création de la Société de Gestion du patrimoine immobilier (SOPIEG).
- Création de la compagnie de l'engineering de l'électricité et du Gaz (CEEG).
- Création de la société des systèmes d'information (ELIT).

➢ En 2010

- Intégration de l'AMC à la fin de l'année 2010.

➢ En 2013

- Création de la Société de production « Shariket Kahraba oua Takat Moutadjadida » SKTM, chargée des réseaux isolés du sud et des Energies Renouvelables, en avril 2013.

➢ En 2014

- Restructuration de la SPAS en 4 sociétés régionales en novembre 2014 : SWAT, SAH, SAR et SAT,

Nouvelle organisation de la maison mère par la création de 04 pôles d'activités et le renforcement du rôle de la DCH, notamment par l'intégration de l'activité organisation, décembre 2014.

I.3.11. Nouvelle stratégie pour de nouveaux horizons en 2020/2021

Le nouveau plan stratégique, dénommé SONELGAZ 2035, redéfinit les missions du Groupe en tant qu'énergéticien axé sur la fourniture d'une énergie fiable et responsable, la prestation de services publics de qualité, et la contribution au bien-être des clients et au développement durable. Pour mettre en œuvre cette stratégie, une nouvelle organisation est instaurée sur deux niveaux : Au niveau Groupe, deux holdings sont créées, détenues à 100 % par SONELGAZ [2]. Une holding Engineering et Construction supervisant les sociétés travaux et d'engineering, et une holding Industries supervisant les sociétés spécialisées dans divers secteurs. La fusion de trois sociétés de protection et de surveillance en une seule, gérée par la SWAT. Au niveau Holding, les pôles d'activités sont transformés en directions exécutives, regroupant les sociétés par métier et activité [2].

I.4. Présentation d'ELIT

I.4.1. Présentation

Le 1er janvier 2009, l'activité des Systèmes d'Information de SONELGAZ a été transformée en une société par actions nommée "EL Djazair Information Technology" (ELIT Spa).

En tant que filiale du Groupe SONELGAZ, ELIT vise à mettre en place un système d'information intégré pour l'ensemble du groupe et le marché national. Avec une croissance dynamique et une stratégie ambitieuse, ELIT s'engage dans une gestion proactive des ressources humaines pour anticiper les besoins en compétences.

La création de ELIT s'inscrit dans la restructuration de SONELGAZ, visant à rationaliser les ressources et les services pour des économies d'échelle. ELIT offre une gamme étendue de services en technologies de l'information et de la communication, incluant la conception, le développement, l'intégration, la maintenance des logiciels, la gestion des réseaux informatiques et téléphoniques, ainsi que des services d'accompagnement et de formation.

Cette initiative est essentielle dans la stratégie de modernisation et d'optimisation des opérations informatiques de SONELGAZ, tout en générant des économies et en améliorant l'efficacité globale de l'entreprise [3].

I.4.2. Structure de ELIT

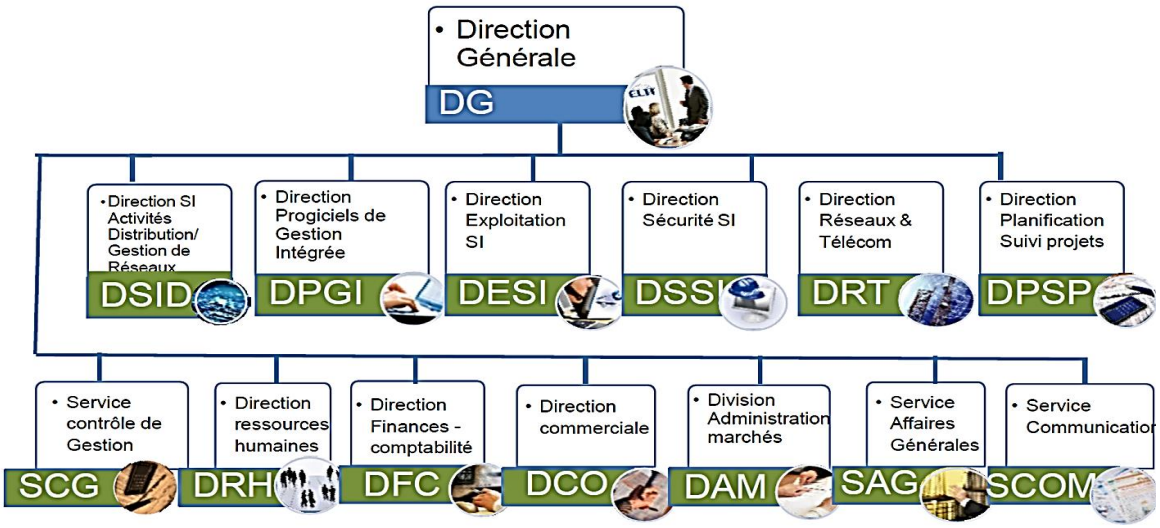


Figure I.3. Organigramme d'ELIT [2].

I.4.3. Mission et attributions de la Société

La société EL Djazair information Technology- ELIT SPA, est de chargée de définir et de mettre en œuvre la politique générale du Groupe SONELGAZ concernant les systèmes d'information et les technologies de l'information et de la communication.

- Elaborer le schéma Directeur SI du Groupe SONELGAZ.
- Elaborer et mettre en œuvre les systèmes d'information destines au pilotage et à la gestion des différentes activités du Groupe SONELGAZ.
- Mettre à la disposition du Groupe SONELGAZ les moyens informatiques et de télécommunications (ressources, matériels, infrastructures, etc.) nécessaires pour assurer le niveau de service attendu.
- Assurer des prestations en termes de besoins en systèmes d'information par la fourniture de services en mode client/ fournisseur.
- Veiller au choix des normes, des standards et des méthodes, a des fins d'optimisations économique et technique et de faciliter l'interopérabilité et les échanges d'informations, des plates-formes et des équipements mis à la disposition des utilisateurs.
- Assurer l'accès à l'information et aux applications et en garantir la sécurité, l'intégrité et la fiabilité.

Assurer le rôle de centre d'expertise du Groupe par le développement des ressources humaines et des méthodologies adaptées, proposer à terme ces mêmes services aux clients externes.

I.4.4. Organigramme de DRT

La Direction Réseaux et Télécoms (DRT) de SONELGAZ est chargée de développer, mettre en œuvre et maintenir les moyens de communication nécessaires au déploiement des systèmes d'information, ainsi que de fournir les services requis pour améliorer les échanges d'informations au sein du groupe et de ses filiales.

Ses principales attributions comprennent :

- L'étude des normes et standards pour l'évolution cohérente des systèmes de communication.
- La validation des solutions technologiques, l'optimisation des coûts télécoms, la sélection des partenaires et l'intégration de nouvelles technologies telles qu'Internet,

la VOIP et les solutions mobiles.

- Elle est également responsable du développement, de la maintenance et de l'administration des réseaux informatiques et téléphoniques, ainsi que de l'assistance technique et de l'administration des réseaux du groupe.
- En outre, elle planifie et optimise la capacité du réseau, définit les principes et les modèles de solutions de réseaux sans fil et de technologies mobiles.
- Elle assure également le bon fonctionnement des plates-formes réseau et des accès
- Distants des serveurs centralisés.

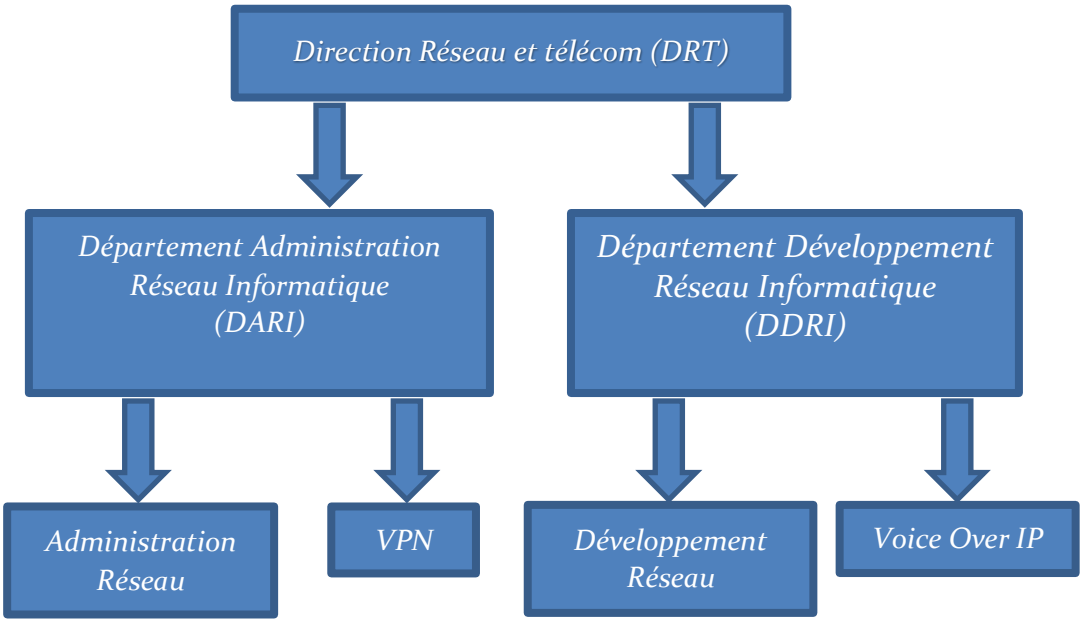


Figure I.4. Organigramme DRT [2].

I.5. Conclusion

En conclusion, ce chapitre a permis de fournir une vue d'ensemble approfondie de l'organisme d'accueil du groupe SONELGAZ. En mettant en lumière son rôle stratégique dans le secteur énergétique, son organisation interne, ainsi que ses missions et objectifs, nous avons pu mieux comprendre le contexte opérationnel dans lequel s'inscrit notre projet de gestion et de supervision des infrastructures VoIP. Cette compréhension approfondie des enjeux spécifiques liés à SONELGAZ est essentielle pour orienter efficacement nos efforts vers l'optimisation des communications et la garantie de la disponibilité des services au sein de cette entité.

Chapitre II
Généralité sur la VoIP

II.1. Introduction

Les systèmes de téléphonie VoIP, plus communément connu sous l'appellation de voix sur IP en français. On les désigne également par les termes de téléphonie IP, téléphonie Internet ou encore appels Internet.

Ces solutions offrent une alternative au réseau téléphonique public commuté (RTC), offrant des avantages significatifs pour les entreprises. Cependant, de nombreux professionnels ne comprennent pas le fonctionnement de la VoIP et méconnaissent les possibilités qu'elle offre en matière de communication.

C'est dans cette optique nous détaillons dans les éléments constitutifs d'un réseau VoIP, ses protocoles et le fonctionnement pratique. Ainsi, vous pourrez appréhender pleinement leur potentiel et découvrir les bénéfices de la téléphonie IP.

II.2. Eléments constitutifs d'un réseau VoIP

II.2.1. Matériel

Pour réaliser une infrastructure de téléphonie, il faut avoir recours à de nombreux éléments matériels, parfois incompatibles ensembles. La prudence s'impose donc avant d'effectuer les investissements nécessaires [4 et 12].

II.2.1.1. PABX-IP

Assure la gestion des appels et leur routage, pouvant également fonctionner comme routeur, switch ou serveur DHCP selon les modèles. Il offre diverses interfaces, telles qu'analogiques (fax), numériques (postes) ou opérateurs (RTC-PSTN ou RNIS). Gérable via IP en Intranet ou par un logiciel serveur dédié, il peut s'interconnecter avec d'autres PABX-IP de la même marque (réseau homogène) ou avec des PABX d'autres marques (réseau hétérogène).

II.2.1.2. Passerelle (Getway)

La passerelle est un dispositif de routage doté de cartes d'interfaces analogiques et/ou numériques permettant de se connecter à d'autres PABX ou à des opérateurs de télécommunications locaux, nationaux ou internationaux. Plusieurs passerelles peuvent être intégrées dans un réseau unique, ou une passerelle peut être dédiée à un réseau local (LAN).

Elle assure également l'interface pour les postes analogiques traditionnels, leur permettant d'utiliser toutes les fonctionnalités du réseau téléphonique IP, y compris les appels internes et externes.

II.2.1.3. IP-Phone

Il s'agit d'un terminal téléphonique opérant sur le réseau LAN IP, conforme aux normes propriétaires, SIP ou H.323. Il peut intégrer plusieurs codecs audios, et être équipé d'un écran monochrome ou couleur ainsi que de touches programmables ou préprogrammées. Généralement, il est équipé d'un hub passif à un seul port pour alimenter l'ordinateur de l'utilisateur, où l'IP PHONE se connecte à la prise Ethernet murale et l'ordinateur se connecte derrière l'IP PHONE.

Un Soft-Phone peut également être utilisé, un logiciel qui gère toutes les fonctions téléphoniques en utilisant la carte son, le micro et la carte Ethernet de l'ordinateur de l'utilisateur. Il peut être géré soit par le Call Manager, soit par le PABX-IP.

II.2.1.4. Routeur

Il assure l'acheminement des paquets d'un réseau vers un autre réseau.

II.2.1.5. Switch

Il assure la distribution et la commutation de dizaines de port Ethernet à 10/100 voire 1000 Mbits/s. Suivant les modèles, il peut intégrer la télé alimentation des ports Ethernet à la norme 802.3af pour l'alimentation des IP-phones ou des bornes WIFI en 48V.

II.2.1.6. Gatekeeper

Il effectue les translations d'adresses et gère la bande passante et les droits d'accès. C'est le point de passage obligé pour tous les équipements de sa zone d'action.

II.2.1.7. MCU

Un multipoint control unit (MCU) est un logiciel informatique ou une machine servant à établir simultanément plusieurs communications de visioconférence ou de VoIP.

II.2.2. Logiciels

Ce sont les produits qui stockent la configuration des utilisateurs, le plan de numérotation (la logique de routage des appels), les messageries vocales... et qui réalisent le routage des appels. Parmi cette catégorie, nous trouvons de nombreux produits parmi lesquels (liste bien entendu non exhaustive) [4] :

Autocoms propriétaires

- OmniPCX (Alcatel- Lucent).
- NexSpan (Aastra Matra, ex EADS télécoms).
- Call Manager (Cisco).
- Media Gateway (Avaya).
- Autres constructeurs : Ericsson, Mitel, 3Com, Nortel.

Autocoms Open Source

- Asterisk.
- SipX (www.sipfoundry.org) : beaucoup de fonctionnalités autour des communications unifiées (conférences, trunk sip, IVR, gestion de présence, vidéo…).
- Elastix (www.elastix.org): appliance ready-to-use.
- My SIPSwitch (www.mysipswitch.com) et son successeur Sipsorcery (sipsorcery.codeplex.com) en version bêta (février 2010).

Opérateurs télécoms

- Orange.
- SFR (ex 9 Telecom/Cegetel).
- Autres opérateurs : Bouygues, Free, Completel, Altitude Telecom, Futur Telecom...

Autres opérateurs alternatifs : toute entreprise peut monter un business d'opérateur télécom et de passerelles voix, en partant d'offres des grands opérateurs en marque blanche ou en construisant ses propres « briques ». La demande du statut d'opérateur est à soumettre à l'ARCEP (Autorité de Régulation des Télécoms). Le statut n'est pas compliqué à obtenir mais il faut savoir que cela nécessite une tâche administrative à budgéter ainsi qu'une taxe qui est fonction du chiffre d'affaires [4].

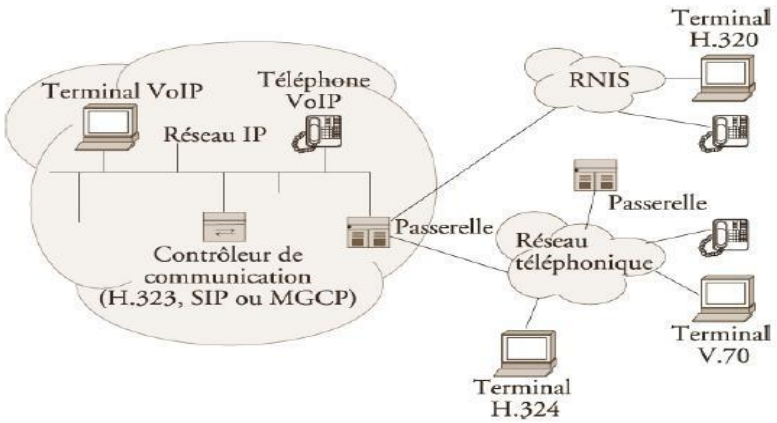


Figure II.1. Schéma général de l'utilisation de la VoIP [12].

II.3. Protocoles de la VoIP

Un protocole est une norme formalisée qui facilite la communication entre différents processus. Il représente un ensemble de règles et de procédures pour l'échange de données sur un réseau. Dans le domaine des télécommunications et des réseaux, chaque application utilise son propre protocole. Le protocole le plus connu et le plus largement utilisé est le TCP/IP (Transmission Control Protocol/ Internet Protocol).

L'un des principaux défis de la VoIP (Voice over Internet Protocol) est de convertir un flux audio en données numériques, en le fragmentant en paquets pour qu'il puisse être transmis sur les réseaux IP. Il est également essentiel de réaliser cette opération dans le bon ordre afin que l'interlocuteur puisse comprendre clairement le flux audio en temps réel, avec un délai inférieur à 300 millisecondes [4].

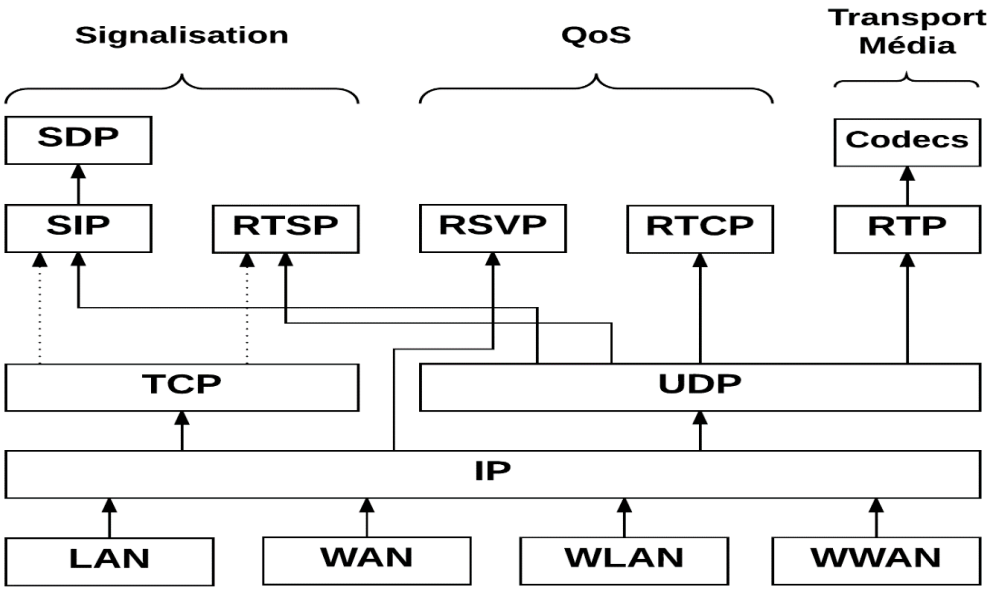


Figure II.2. Protocoles de VoIP [13].

II.3.1. Protocoles de signalisation

Un protocole de signalisation est un mécanisme de la couche 5 (Session) du modèle OSI qui gère la communication téléphonique IP selon les étapes suivantes :

- L'appelant spécifie les coordonnées de la personne qu'il souhaite contacter en composant le numéro.
- Le correspondant est informé de l'appel entrant (sonnerie de son téléphone).
- Le correspondant accepte l'appel (décroche son téléphone).
- Les tiers tentant de contacter les deux interlocuteurs sont informés de leur indisponibilité (ligne occupée).
- La communication se termine et les lignes redeviennent disponibles (raccrochage).
- Les principaux protocoles utilisés pour établir des connexions téléphoniques sur IP sont :
    - H.323
    - SIP
    - MGCP
    - IAX (utilisé par Asterisk) [5].

II.3.1.1 Protocole H.323

Le standard H.323, fournit depuis son approbation en 1996, un cadre pour les communications audio, vidéo et de données sur les réseaux IP. Il a été développé par l'ITU (International Télécommunications Union) pour les réseaux qui ne garantissent pas une QoS (Quality of service), tels que FastEthernet et Token Ring. Il est présent dans plus de 30 produits. H.323 concerne le contrôle des appels, la gestion multimédia, la gestion de la bande passante pour les conférences point-à-point et multipoints. Il traite également de l'interfaçage entre le LAN (Local Area Network) et les autres réseaux.

Le protocole H.323 fait partie de la série H.32x qui traite de la vidéoconférence au travers différents réseaux. Il inclue H.320 et H.324 liés aux réseaux ISDN (Integrated Service Data Network) et PSTN (Public Switched Telephone Network). Plus qu'un protocole, H.323 crée une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories : la signalisation, la négociation de codec, et le transport de l'information.

Les messages de signalisation sont ceux envoyés pour demander la mise en relation de deux clients, qui indique que la ligne est occupée ou que le téléphone sonne, etc. Avec H.323, la

Signalisation s'appuie sur le protocole RAS (Registration/Admission/Status) pour l'enregistrement et l'authentification, et le protocole Q.931 pour l'initialisation et le contrôle d'appel.

Une communication H.323 se déroule en cinq phases : l'établissement d'appel, l'échange de capacité et réservation éventuelle de la bande passante à travers le protocole RSVP (Ressource Réservation Protocol), l'établissement de la communication audio-visuelle, l'invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante, etc.) et enfin la libération de l'appel [6].

i. Les composants de H.323

La figure II.3 représente l'infrastructure H.323 qui se repose sur quatre composants principaux : les terminaux, les Gateways, les Gatekeepers, et les MCU (Multipoint Control Units).

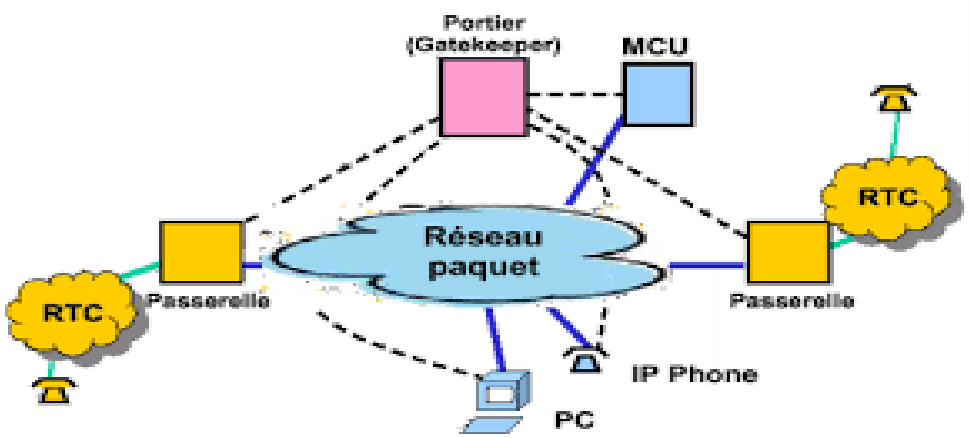


Figure II.3. Les composants de l'architecture H.323 [14].

ii. Les terminaux H.323

Le terminal : peut-être un ordinateur, un combiné téléphonique, un terminal spécialisé pour la vidéoconférence ou encore un télécopieur sur Internet. Le minimum imposé par H.323 est qu'il mette en œuvre la norme de compression de la parole G.711, qu'il utilise le protocole H.245 pour la négociation de l'ouverture d'un canal et l'établissement des paramètres de la communication, ainsi que le protocole de signalisation Q.931 pour l'établissement et l'arrêt des communications. Le terminal possède également des fonctions optionnelles, notamment, pour le travail en groupe et le partage des documents. Il existe deux types de terminaux H.323, l'un de haute qualité (pour une utilisation sur LAN), l'autre optimisé pour de petites largeurs de bandes (28,8/33,6 kbit/s – G.723.1 et H.263).

Gateway ou les passerelles vers des réseaux classiques (RTC, RNIS, etc.) : Les passerelles H.323 assurent l'interconnexion avec les autres réseaux, ex : les modems H.324, les téléphones classiques, etc. Elles assurent la correspondance de signalisation de Q.931, la correspondance des signaux de contrôle et la cohésion entre les medias (multiplexage, correspondance des débits, transcodage audio).

Gatekeeper ou les portiers : Dans la norme H.323, Le Gatekeeper est le point d'entrée au réseau pour un client H.323. Il définit une zone sur le réseau, appelée zone H.323 (voir Figure1.3), regroupant plusieurs terminaux, Gateways et MCU dont il gère le trafic, le routage LAN, et l'allocation de la bande passante. Les clients ou les Gateway s'enregistrent auprès du Gatekeeper dès l'activation de celui-ci, ce qui leur permet de retrouver n'importe quel autre utilisateur à travers son identifiant fixe, obtenu auprès de son Gatekeeper de rattachement.

Le Gatekeeper a pour fonction :

- La translation des alias H.323 vers des adresses IP, selon les spécifications RAS (Registration/Admission/Status).
- Le contrôle d'accès, en interdisant les utilisateurs et les sessions non autorisés.
- La gestion de la bande passante, permettant à l'administrateur du réseau de limiter le nombre de visioconférences simultanées. Concrètement, une fraction de la bande passante est allouée à la visioconférence, pour ne pas gêner les applications critiques sur le LAN et le support des conférences multipoint Adhoc.

Les MCU (Multipoint Control Unit) : Les contrôleurs multipoint appelés MCU offrent aux utilisateurs la possibilité de faire des visioconférences à trois terminaux et plus en « présence continue » ou en « activation à la voix ». Une MCU consiste en un Contrôleur Multipoint (MC), auquel est rajouté un ou plusieurs Processeurs Multipoints (MP). Le MC prend en charge les négociations H.245 entre tous les terminaux pour harmoniser les paramètres audio et vidéo de chacun. Il contrôle également les ressources utilisées. Mais le MC ne traite pas directement avec les flux audio, vidéo ou données, c'est le MP qui se charge de récupérer les flux et de leurs faire subir les traitements nécessaires. Un MC peut contrôler plusieurs MP distribués sur le réseau et faisant partie d'autres MCU [6].

iii. Avantages et inconvénients de la technologie H.323

La technologie H.323 possède des avantages et des inconvénients. Parmi les avantages, nous citons [6] :

- Gestion de la bande passante : H.323 permet une bonne gestion de la bande passante en posant des limites au flux audio/vidéo afin d'assurer le bon fonctionnement des applications critiques sur le LAN. Chaque terminal H.323 peut procéder à l'ajustement de la bande passante et la modification du débit en fonction du comportement du réseau en temps réel (latence, perte de paquets et gigue).
- Support Multipoint : H.323 permet de faire des conférences multipoint via une structure centralisée de type MCU (Multipoint Control Unit) ou en mode ad-hoc.
- Support Multicast : H.323 permet également de faire des transmissions en multicast.
- Interopérabilité : H.323 permet aux utilisateurs de ne pas se préoccuper de la manière dont se font les communications, les paramètres (les codecs, le débit...) sont négociés de manière transparente.
- Flexibilité : une conférence H.323 peut inclure des terminaux hétérogènes (studio de visioconférence, PC, téléphones…) qui peuvent partager selon le cas, de la voix de la vidéo et même des données.

Les inconvénients de la technologie H.323 sont [6] :

- La complexité de mise en œuvre et les problèmes d'architecture en ce qui concerne la convergence des services de téléphonie et d'Internet, ainsi qu'un manque de modularité et de souplesse.
- Comprend de nombreuses options susceptibles d'être implémentées de façon différente par les constructeurs et donc de poser des problèmes d'interopérabilité.

II.3.1.2. Protocole SIP

Le Session Initiation Protocol (SIP) est un protocole de couche application du TCP/IP, normalisé et standardisé par l'IETF via le RFC 3261. Son objectif principal est de mettre en place, modifier et clôturer des sessions multimédia. SIP gère l'authentification et la localisation de plusieurs participants. Bien qu'il soit responsable de la négociation des médias, il délègue le transport du texte, de la voix ou de la vidéo à d'autres protocoles.

SIP est compatible avec IPv4 et IPv6. Il peut être utilisé avec TCP ou UDP sur le port

5060 par défaut. La version sécurisée, SIP-TLS, utilise le port TCP 5061 par défaut.

SIP gère cinq aspects essentiels de l'établissement et de la fin de communications multimédia :

- Localisation de l'utilisateur **:** identification du terminal à utiliser pour la communication.
- Disponibilité de l'utilisateur **:** évaluation de la disposition de l'appelé à participer à une communication. Capacités de l'utilisateur : identification du support et des paramètres de support à utiliser.
- Etablissement de session **:** mise en place des paramètres de session pour l'appelant et l'appelé, incluant la "sonnerie".
- Gestion de session **:** incluant le transfert, la fin des sessions, la modification des paramètres de session et l'invocation des services.

SIP n'est pas une solution de communication intégrée verticalement. Il s'agit plutôt d'un composant qui peut être combiné avec d'autres protocoles de l'IETF pour construire une architecture multimédia complète.

Contrairement à fournir directement des services, SIP offre des primitives utilisables pour mettre en place divers services. Par exemple, SIP peut localiser un utilisateur et transmettre un objet opaque à son emplacement. Une seule primitive peut souvent servir à plusieurs services distincts.

La nature des services offerts par SIP rend la sécurité particulièrement cruciale. À cet égard, SIP propose une gamme de services de sécurité, incluant la prévention des attaques par déni de service, l'authentification (entre utilisateurs et entre mandataires et utilisateurs), la protection de l'intégrité, ainsi que des services de chiffrement et de confidentialité [7].

i. Les composants de SIP

SIP est basé sur un User Agent (UA), un registrar et un proxy.

UAC : Un Agent Utilisateur Client est tout élément de réseau qui envoie une requête SIP et reçoit des réponses SIP. Les clients peuvent ou non interagir directement avec un utilisateur humain. Les clients et proxys d'UA sont des clients.

UAS : Un Agent Utilisateur Serveur est une entité logique qui génère une réponse à une requête SIP. La réponse accepte, rejette, ou redirige la requête. Ce rôle ne dure que pendant le temps de cette transaction. En d'autres termes, si un logiciel répond à une requête, il agit comme UAS pour la durée de cette transaction. S'il génère plus tard une requête, il assume le rôle d'un UAC

pour le traitement de cette transaction.

Proxy : Serveur Proxy (ou serveur mandataire) : C'est une entité intermédiaire agissant à la fois comme un serveur et comme un client pour traiter les requêtes au nom d'autres clients.

Le rôle principal d'un serveur proxy est d'acheminer et de router les requêtes, garantissant ainsi qu'elles sont dirigées vers une entité "plus proche" de l'utilisateur cible. Il fonctionne de manière similaire à un routeur IP qui oriente le trafic en se basant sur l'adresse IP de destination.

Les Proxy sont également utiles pour appliquer des politiques de routage des appels, comme vérifier si un utilisateur est autorisé à passer un appel [7].

ii. Le fonctionnement de SIP

Requêtes SIP : Le client envoie des requêtes au serveur ; serveur qui, en retour, lui renvoie une réponse.

Les méthodes de base comprises dans ces requêtes sont :

- INVITE : permet à un client de demander une nouvelle session,
- ACK : confirme l'établissement de la session,
- CANCEL : annule un INVITE en suspens,
- BYE : termine une session en cours,
- OPTIONS : permet de récupérer les capacités de gestion des usagers, sans ouvrir de session,
- REGISTER : permet de s'enregistrer auprès d'un serveur d'enregistrement.
- Réponses (Status Codes) SIP **:** Selon le contexte, une réponse est attendue lors d'une transaction, et les réponses possibles sont similaires à celles des codes http Idéalement, une réponse "200 OK" indique une réussite.
- Une transaction SIP se déroule entre un client et un serveur et englobe tous les messages, de la première requête du client au serveur jusqu'à la réponse finale (hors codes 1xx) du serveur au client. Si la requête est un "INVITE" et que la réponse finale n'est pas un code "2xx", la transaction inclut également un "ACK" en réponse. Pour une réponse "2xx" à une requête "INVITE", le "ACK" est traité comme une transaction distincte.
- Un dialogue est une relation SIP bilatérale qui persiste pendant un certain laps de temps entre deux agents utilisateurs. Ce dialogue est initié par des messages SIP, tels

qu'une réponse "2xx" à une requête "INVITE".

- Un dialogue est identifié par un identifiant d'appel, une étiquette locale, et une étiquette distante :
  - Provisionnel (1xx) : La requête est reçue et est en cours de traitement.
  - Succès (2xx) : L'action a été reçue, comprise et acceptée avec succès.
  - Redirection (3xx) : Une action supplémentaire doit être prise (par l'appelant) pour compléter la requête.
  - Client Error (4xx) : La requête comporte une mauvaise syntaxe et ne peut être prise en charge par le serveur.
  - Server Error (5xx) : Le serveur a échoué remplir une requête apparemment valide.
  - Global Failure (6xx) : La requête ne peut être prise en charge par aucun serveur.

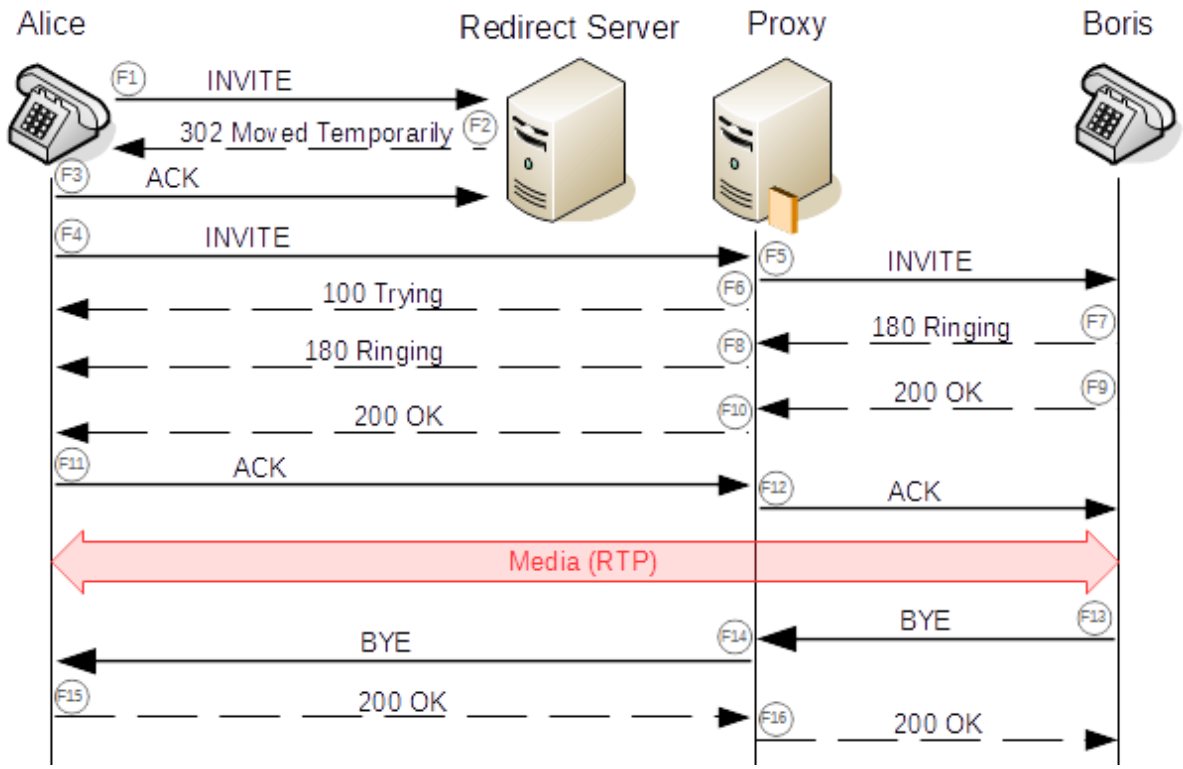


Figure II.4. Fonctionnement de protocole SIP [15].

iii. Avantages et inconvénients de SIP

Les principaux avantages du protocole SIP sont [6] :

- Ouvert : Les protocoles et documents officiels sont détaillés et accessibles à tous en téléchargement.
- Standard : L'IETF a normalisé le protocole et son évolution continue par la création où

l'évolution d'autres protocoles qui fonctionnent avec SIP.

- Simple : SIP est simple et très similaire à http.
- Flexible : SIP est également utilisé pour tout type de sessions multimédia (voix,vidéo, mais aussi musique, réalité virtuelle, etc.).
- Téléphonie sur réseaux publics : Il existe de nombreuses passerelles (services payants) vers le réseau public de téléphonie (RTC, GSM, etc.) permettant d'émettre ou de recevoir des appels vocaux.
- Points communs avec H323 : L'utilisation du protocole RTP et quelques codecs son et vidéo sont en commun.

Parmi ses inconvénients :

- Une implémentation incomplète du protocole SIP dans les User Agents peut perturber le fonctionnement ou générer du trafic superflu sur le réseau [7].
- Le protocole SIP connaît des difficultés à traverser les équipements équipés de mécanisme de NAT (Network Adresse Translation) comme les firewalls et les routeurs. En effet, SIP encapsule toutes les données comprenant les adresses IP, alors que le NAT a besoin de ces informations afin de faire passer les paquets. Les communications sont alors bloquées par le firewall [4].

II.3.1.3. Protocole IAX

C'est le protocole de signalisation de voix/ vidéo sur IP utilisé par Asterisk (Inter Asterisk eXchange). Ce protocole fonctionne sur le port 4569 en UDP et transporte à la fois les données (voix) et la signalisation. L'intérêt principal de ce protocole est d'être fait pour traverser le NAT (Network Address Translation) et qu'il est possible de créer des trunks IAX (trames sont marquées ou taguées pour que les commutateurs sachent à quel Vlan elles appartiennent) entre les serveurs dans lesquels les communications RTP sont multiplexées ainsi on économise les surcharges d'entêtes IP [8].

II.3.1.4. Protocole MGCP

Le protocole MGCP (Media Gateway Control Protocol) est spécifié par la RFC 2705. Il fonctionne sur un modèle où un agent d'appel contrôle le point de terminaison, tandis qu'un Call Agent supervise l'ensemble du processus de contrôle, indiquant au terminal les actions à entreprendre en réponse à certains événements. MGCP utilise les ports TCP 2428 et UDP 2427

pour la communication.

Le port TCP 2428 de MGCP sert à établir un nouveau socket avec l'agent d'appel, vérifiant ainsi la possibilité d'établir une connexion. Sans ce socket initial, les échanges de messages MGCP ultérieurs ne peuvent avoir lieu. Ce port est aussi utilisé pour la transmission de messages de liaison entre les terminaux PRI et l'agent d'appel associé. En cas de défaillance de l'agent d'appel principal, le port TCP 2428 permet également un basculement d'urgence vers un agent de sauvegarde.

Quant au port UDP 2427, il est dédié à la transmission des messages MGCP entre les terminaux et les agents d'appel [9].

II.3.2. Protocoles de transport

Les protocoles de transport de VoIP sont des protocoles qui permettent le transport de la voix sur un réseau IP. Les principaux protocoles de transport de VoIP sont TCP, UDP, RTP et RTCP.

II.3.2.1. Protocole TCP

Les protocole TCP (Transmission Control Protocol) est un des principaux protocoles de la couche transport du modèle OSI. Il permet, au niveau des applications, de gérer les données en provenance de la couche inférieure du modèle (protocole IP).

Lorsque les données sont fournies au protocole IP, celui-ci les encapsule dans des datagrammes IP. Le protocole TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission.

Le protocole TCP permet principalement de :

- Remettre en ordre les datagrammes en provenance du protocole IP
- Vérifier le flux de données afin d'éviter une saturation du réseau
- Formater les données en segments de longueur variable afin de les remettre au protocole IP
- Permet aussi de multiplexer les données [10].

II.3.2.2. Protocole UDP

Contrairement aux données où le débit global est la principale préoccupation, la voix nécessite un flux régulier pour garantir une qualité sonore optimale. Afin de maintenir un trafic

Fluide, l'utilisation de protocoles de transport simplifiés est préconisée, même si cela implique de sacrifier la gestion des erreurs. En effet, la voix est relativement tolérante aux erreurs comparativement aux données, mais sa qualité perçue est fortement influencée par les variations de délai causées par les congestions réseau. Le protocole UDP opère sur la même couche que TCP, mais offre des performances légèrement inférieures en comparaison à ce dernier. Cela est dû à la nature d'UDP qui permet l'envoi de paquets sans mécanisme de contrôle de réception [10].

II.3.2.3. Protocole RTP

RTP (Real time Transport Protocol), standardisé en 1996, est un protocole qui a été développé par l'IETF, afin de faciliter le transport temps réel de bout en bout, des flots donnés audio et vidéo, sur les réseaux IP. RTP est un protocole qui se situe au niveau de l'application et qui utilise les protocoles sous-jacents de transport TCP ou UDP. Mais l'utilisation de RTP se fait généralement au-dessus d'UDP, ce qui permet d'atteindre plus facilement le temps réel. Les applications en temps réels, comme la parole numérique ou la visioconférence constitue un véritable problème pour Internet. Une application en temps réel, exige une certaine qualité de service (QoS) que RTP ne garantit pas du fait qu'il fonctionne au niveau Applicatif.

De plus RTP est un protocole qui se trouve dans un environnement multipoint, donc on peut dire que RTP possède à sa charge, la gestion du temps réel, mais aussi l'administration de la session multipoint [6].

- **Les fonctions de RTP**

Le protocole RTP a pour but d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie. Ceci de façon à reformer les flux avec ses caractéristiques de départ.

RTP est un protocole de bout en bout, volontairement incomplet et malléable pour s'adapter aux besoins des applications. Il sera intégré dans le noyau de l'application. Il laisse la responsabilité du contrôle aux équipements d'extrémité. Il est aussi un protocole adapté aux applications présentant des propriétés temps réel. Il permet ainsi de :

- Mettre en place un séquencement des paquets par une numérotation et ce afin de permettre ainsi la détection des paquets perdus. Ceci est un point primordial dans la reconstitution des données. Mais il faut savoir quand même que la perte d'un paquet n'est

pas un gros problème si les paquets ne sont pas perdus en trop grands nombres.

Cependant il est très important de savoir quel est le paquet qui a été perdu afin de pouvoir pallier à cette perte.

- Identifier le contenu des données pour leurs associer un transport sécurisé et reconstituer la base de temps des flux (horodatage des paquets : possibilité de resynchronisation des flux par le récepteur).
- L'identification de la source c'est à dire l'identification de l'expéditeur du paquet. Dans un multicast l'identité de la source doit être connue et déterminée.
- Transporter les applications audio et vidéo dans des trames (avec des dimensions qui sont dépendantes des codecs qui effectuent la numérisation). Ces trames sont incluses dans des paquets afin d'être transportées et doivent, de ce fait, être récupérées facilement au moment de la phase de segmentation des paquets afin que l'application soit décodée correctement [6].

■ **Avantages et inconvénients**

Le protocole RTP permet de reconstituer la base de temps des différents flux multimédia (audio, vidéo, etc.) ; de détecter les pertes de paquets ; et d'identifier le contenu des paquets pour leur transmission sécurisée. Par contre, il ne permet pas de réserver des ressources dans le réseau ou d'apporter une fiabilité dans le réseau. Ainsi il ne garantit pas le délai de livraison [6].

II.3.2.4. Protocole RTCP

Le protocole RTCP (Real-time Transport Control Protocol) est fondé sur la transmission périodique de paquets de contrôle à tous les participants d'une session. C'est le protocole UDP (par exemple) qui permet le multiplexage des paquets de données RTP et des paquets de contrôle RTCP.

Le protocole RTP utilise le protocole RTCP, qui transporte les informations supplémentaires suivantes pour la gestion de la session. Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS. Ces rapports comprennent le nombre de paquets perdus, le paramètre indiquant la variance d'une distribution (plus communément appelé la gigue : c'est à dire les paquets qui arrivent régulièrement ou irrégulièrement) et le délai aller-retour. Ces informations permettent à la source de s'adapter, par exemple, de modifier le niveau de compression pour maintenir une QoS [6].

- **Les fonctions de RTCP**

Parmi les principales fonctions qu'offre le protocole RTCP, nous citons :

- Une synchronisation supplémentaire entre les médias : Les applications multimédias sont souvent transportées par des flots distincts. Par exemple, la voix, l'image ou même des applications numérisées sur plusieurs niveaux hiérarchiques peuvent voir les flots gérés et suivre des chemins différents.
- L'identification des participants à une session : En effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.
- Le contrôle de la session : En effet le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement de fournir une indication sur leur comportement.
- SR (Sender Report) : Ce rapport regroupe des statistiques concernant la transmission (pourcentage de perte, nombre cumulé de paquets perdus, variation de délai (gigue), etc.). Ces rapports sont issus d'émetteurs actifs d'une session.
- RR (Receiver Report) : Ensemble de statistiques portant sur la communication entre les participants. Ces rapports sont issus des récepteurs d'une session.
- SDES (Source Description) : Carte de visite de la source (nom, e-mail, localisation).
- BYE : Message de fin de participation à une session.
- APP : Fonctions spécifique à une application [6].

- **Avantages et inconvénients**

Le protocole de RTCP est adapté pour la transmission de données temps réel. Il permet d'effectuer un contrôle permanant sur une session et ces participants. Par contre il fonctionne en stratégie bout à bout. Et il ne peut pas contrôler l'élément principal de la communication " le réseau " [6].

II.3.3. Protocoles de codec

Le terme "codec" est dérivé de la fusion des mots "codage" et "décodage", et il est utilisé pour traiter les données audios numériques. Un codec est un logiciel qui convertit les données numériques en un format de fichier audio ou en un format de flux audio. Il permet de transformer un signal vocal analogique en un signal vocal numérique. Les variations entre les codecs concernent la qualité audio, la bande passante nécessaire à leur utilisation et les

exigences du système en matière d'encodage [11].

Lorsque vous utilisez un téléphone traditionnel sur le réseau téléphonique commuté (RTC), votre voix est transmise sous forme analogique via la ligne téléphonique. En revanche, avec la voix sur IP (VoIP), votre voix est convertie en signaux numériques. Cette conversion est appelée encodage et est réalisée par un codec. Une fois que la voix encodée atteint son destinataire, elle doit être décodée en format analogique d'origine pour que la personne qui reçoit l'appel puisse entendre et comprendre l'appelant.

Il existe de nombreux codecs disponibles pour la VoIP, chacun ayant ses propres caractéristiques en termes de taux de compression, vitesse de compression et décompression, consommation de CPU et mémoire, qualité du signal de sortie [11].

Les codecs les plus couramment utilisés en VoIP sont :

- **G 711 :** Dans Asterisk, le codec portant le nom de ulaw (µ-law) est utilisé en Amérique du Nord, tandis que le codec alaw est utilisé dans le reste du monde, y compris en France. Le codec G.711 alaw consomme une bande passante de 64 kbps (en prenant en compte l'overhead associé aux flux RTP), mais nécessite peu de ressources CPU car il est presque non compressé.

  Sa qualité est excellente, comparable à celle de la téléphonie RTC traditionnelle. Ce codec est particulièrement adapté pour les réseaux locaux (LAN) où la bande passante n'est généralement pas un problème majeur. Un autre avantage du G.711 est sa disponibilité gratuite et son intégration dans la plupart des équipements de téléphonie sur IP (T-VoIP) [4].

- **G 723.1** : Ce codec payant est utilisé uniquement en cas de transcodage, G.7231 fonctionne à 5,3 Kb/s ou 6,3 Kb/s donc est très intéressant dans le cas de faibles bandes passantes [4].
- **G726 :** Il s'agit d'un codec gratuit qui utilise différents débits : 16, 24 ou 32 Kb/s. Il est supporté par Asterisk uniquement dans sa version 32 bits. C'est un très bon rapport qualité sonore/utilisation CPU [4].
- **G 729 :** Ce codec réduit la consommation d'un appel à 8 Kb/s, auquel s'ajoute l'overhead IP, portant le débit réel à environ 40 Kb/s. Le principal avantage du G.729, utilisé avec Asterisk,est la réduction significative de la bande passante nécessaire, offrant ainsi des gains appréciables. Asterisk prend en charge uniquement le G.729 Annexe A (G.729a) [4].

L'overhead IP varie en fonction de la configuration matérielle du serveur. Par exemple, un processeur Xeon 1.8 GHz peut gérer environ 60 appels simultanés en G729, tandis qu'un Xeon 2.8 GHz peut en gérer 80.

La licence G.729 est payante et doit être installée sur le serveur Asterisk. Une licence est requise pour chaque communication utilisant le transcodage. Si le serveur ne réalise pas de transcodage, aucune licence n'est nécessaire.

Toutefois, si le serveur effectue le codage/décodage (par exemple, client en G711a, Asterisk en G711a/G729, opérateur en G729), une licence est nécessaire pour chaque communication simultanée souhaitée. Bien que ce codec offre des performances remarquables, il consomme considérablement les ressources processeur du serveur.

Pour supporter 30 communications simultanées en G729 sur Asterisk, l'achat d'un pool de 30 licences est nécessaire, ce qui représente environ 300 $ US. Chaque pool de licences est spécifique à un serveur Asterisk [4].

- **GSM :** Est le codec d'Asterisk et ne requiert pas de licences. Il utilise une bande passante intéressante de 13 Kbps, consomme beaucoup moins de ressource processeur que G.729a, tout en étant très performant. Seul inconvénient, le son peut s'avérer de moins bonne qualité que celui avec G.729a [4].

II.4. ToIP

ToIP (Telephony over Internet Protocol) est un service de communication public ou privé qui utilise le protocole de réseau Internet (IP). La technologie ToIP convertit la voix en données via le protocole IP. Ces données sont ensuite diffusées sur le réseau local et retranscrites en parole pour être envoyées à l'interlocuteur. La technologie ToIP permet de s'appuyer sur l'infrastructure réseau IP existante pour connecter des terminaux, des téléphones IP ou des solutions logicielles comme Skype [36].

Le transport de flux vocaux « en direct » sur des réseaux à commutation de paquets peut sembler délicat. Cependant, les débits élevés des réseaux locaux (LAN) et des réseaux étendus (WAN et Internet) permettent de surmonter cette difficulté et de fournir une voix de haute qualité.

La téléphonie sur IP peut :

- S'ajouter en complément sur un réseau téléphonique traditionnel existant.
- S'utiliser en full-IP pour une nouvelle infrastructure.
- S'utiliser en multi sites full-IP avec l'aide d'un opérateur adéquat et de serveurs centralisés.

- S'utiliser sur un ordinateur relié au réseau Internet à destination d'un autre ordinateur relié lui aussi à Internet à l'aide d'un logiciel unique (les communications seront donc gratuites de PC à PC).

II.4.1. Comment fonctionne le téléphone IP

La téléphonie IP fonctionne en convertissant la voix en données numériques pour les transmettre via des réseaux IP, tels qu'Internet. Voici une explication étape par étape du fonctionnement de la téléphonie IP [16].

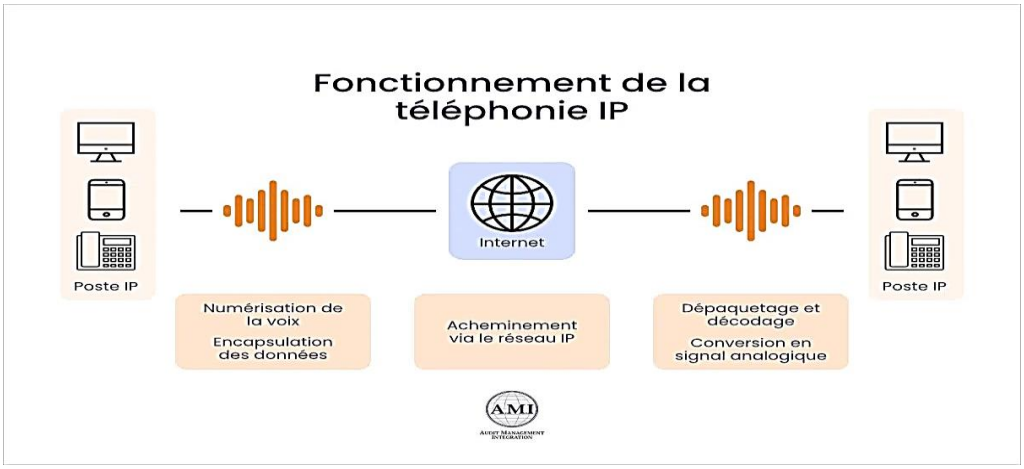


Figure II.5. Schéma descriptif du fonctionnement de la téléphonie IP [16].

- Numérisation de la voix : Lorsqu'un utilisateur effectue un appel via un téléphone IP,un softphone sur un ordinateur ou une application mobile, le microphone du dispositif capte sa voix. Cette voix analogique est ensuite transformée en données numériques grâce à un codec (encodeur/décodeur) [16].
- Encapsulation des données **:** Les données vocales numériques sont divisées en petits paquets d'informations, chacun étant doté d'une adresse de destination (adresse IP du destinataire) et d'une adresse d'origine (adresse IP de l'émetteur). Ces paquets contiennent également des informations de contrôle pour assurer la bonne transmission des données [16].
- Transfert à travers le réseau IP **:** Les paquets de données vocales sont transmis à travers des réseaux IP, comme Internet, en employant le protocole Internet (IP). Ils suivent le chemin le plus rapide et optimal pour arriver à leur point d'arrivée [16].
- Dés encapsulation et décodage **:** À leur arrivée, les paquets de données sont reconstitués dans l'ordre approprié. Les données vocales sont ensuite extraites des paquets et converties en signal vocal [16].

Conversion en signal analogique **:** Finalement, le signal vocal numérique est transformé en signal analogique afin d'être émis par le haut-parleur du téléphone ou de l'appareil du destinataire. De cette manière, le destinataire peut écouter la voix de l'appelant [16].

La VOIP présente de nombreux avantages pour la téléphonie d'entreprise. Elle simplifie l'installation et l'utilisation grâce à des logiciels comme le Softphone, réduisant le temps et la complexité par rapport aux installations traditionnelles. Cette technologie permet des économies significatives sur les appels longue distance et offre une intégration avec vos outils métiers, favorisant une gestion efficace des données et une prise de décision éclairée.

Elle améliore la productivité des collaborateurs en centralisant les informations et en facilitant le suivi commercial et la relation client. La VOIP est également adaptée au travail à distance, éliminant le besoin d'un téléphone fixe et permettant l'accès aux appels et aux données depuis n'importe quel appareil connecté, idéal pour les déplacements professionnels et les appels longue distance à l'étranger.

En outre, la qualité des appels est comparable à celle du service RTC, sous réserve d'un bon SLA de la part de votre opérateur de téléphonie VOIP. Pour une expérience optimale, il est essentiel d'avoir un bon matériel et de s'assurer que votre fournisseur propose une couverture mondiale, des mises à jour régulières et un support expert lors de la mise en œuvre du produit [17].

II.4.2. Différences entre ToIP et VoIP

ToIP et VoIP sont deux technologies similaires mais différentes. Bien que tous deux utilisent le protocole Internet IP, leurs modes de fonctionnement sont différents.

La VoIP convertit la parole en fichier numérique et l'envoie sous forme de paquets sur un réseau de données (tel qu'Internet) via des lignes IP. Il regroupe toutes les technologies qui permettent ce genre de transfert : d'un téléphone IP vers un PC ou un téléphone « classique », ou d'un ordinateur à un autre sur les réseaux internes et externes de l'entreprise.

ToIP est un système téléphonique limité aux réseaux IP locaux. Il crée une connexion entre le réseau LAN (entreprise) et le réseau WAN (opérateur) à l'aide d'un simple routeur : IPBX.
La ToIP regroupe tous les échanges de téléphone IP à téléphone IP, ou d'ordinateur à ordinateur (en utilisant le même logiciel).

Si la ToIP est basée sur VoIP, la VoIP offre des applications et services multiples au-delàs de la simple téléphonie : visioconférence sur IP, messageries vocales unifiées… cette technologie

permet une convergence entre la voix, la vidéo et les données [36].

II.5. Conclusion

La VoIP a révolutionné la communication en offrant une alternative moderne et efficace aux systèmes téléphoniques traditionnels. Ce chapitre a mis en lumière les protocoles et codecs qui permettent cette communication sur les réseaux IP, ainsi que les avantages de la VoIP tels que la simplicité d'installation, les économies sur les appels longue distance et l'intégration avec les outils métiers. Toutefois, des défis comme la nécessité d'une connexion Internet stable et un matériel adéquat ont été soulignés. Pour une expérience optimale, il est crucial de comprendre les composants de la VoIP et de s'assurer d'un soutien fiable de la part des fournisseurs de services.

Chapitre III
Etude et choix de la solution de supervision

III.1. Introduction

Les systèmes Asterisk et les outils de supervision des télécommunications IP jouent un rôle crucial dans la gestion et l'optimisation des réseaux de voix sur IP. Asterisk, un IPBX applicatif open source, permet l'interconnexion en temps réel des réseaux de voix sur IP et des réseaux de téléphonie classique, offrant une vaste gamme de fonctionnalités à moindre coût.

Parallèlement, les systèmes de supervision assurent le bon fonctionnement de l'infrastructure informatique, permettant de détecter et de résoudre rapidement les problèmes pour éviter les interruptions coûteuses des services.

Ce chapitre explore en profondeur les fondements et les fonctionnalités d'Asterisk, les différentes distributions basées sur Asterisk, ainsi que les outils et technologies de supervision, en comparant leurs avantages et inconvénients pour fournir une vue d'ensemble complète de ces systèmes essentiels [36, 37].

III.2. Systèmes Asterisks

Asterisk est un IPBX applicatif open source permettant d'interconnecter en temps réel des réseaux de voix sur IP via plusieurs protocoles (SIP, H323, ADSI, MGCP) et des réseaux de téléphonies classiques via des cartes d'interface téléphonique ou des lignes VOIP, tout ceci à moindre coût.

Asterisk a été initialement écrit par Mark Spencer de Digium, anciennement Linux Support Services, Inc. Les programmeurs Open Source du monde entier ont contribué à l'écriture de la source aux expérimentations, et aux patches correctifs des bugs en provenance de la communauté ont apporté une aide précieuse au développement de ce logiciel. Asterisk offre toutes les fonctions d'un PBX et ses services associés comme de la conférence téléphonique, des répondeurs interactifs, de la mise en attente d'appels, des mails vocaux, de la musique d'attente, de la génération d'enregistrement d'appels pour l'intégration avec des systèmes de facturation. De plus il offre des fonctions avancées comme l'envoi de Voice mails (mail avec le message vocal en pièce jointe), la création de centres d'appels virtuels [18].

III.2.1. Fonctionnalités d'asterisks

Asterisk est en fait un outil de communication. Il a beaucoup de fonctionnalités. Ce qui se produit le plus souvent est un PBX, mais il n'est pas nécessairement un PBX.Cela peut être un logiciel de centre de contact, un distributeur automatique d'appels, un système de messagerie

vocale, un système de courrier vidéo, un IP-PBX, ou bien plus encore. Quelqu'un pourrait même ajouter ses propres crochets IoT pour le transformer en un autre type de système de communication [19].

Figure III.1. Schéma descriptif du Fonctionnalités d'asterisk [19].

III.2.1.1. Appels d'extension à extension

Asterisk offre la possibilité d'effectuer des appels d'extension à extension, permettant aux utilisateurs de composer un numéro d'un téléphone à un autre. Contrairement aux systèmes téléphoniques élémentaires, comme les Key Systems, où les combinés ne disposent pas d'extensions individuelles qui peuvent être composées, Asterisk permet des communications internes dirigées [19].

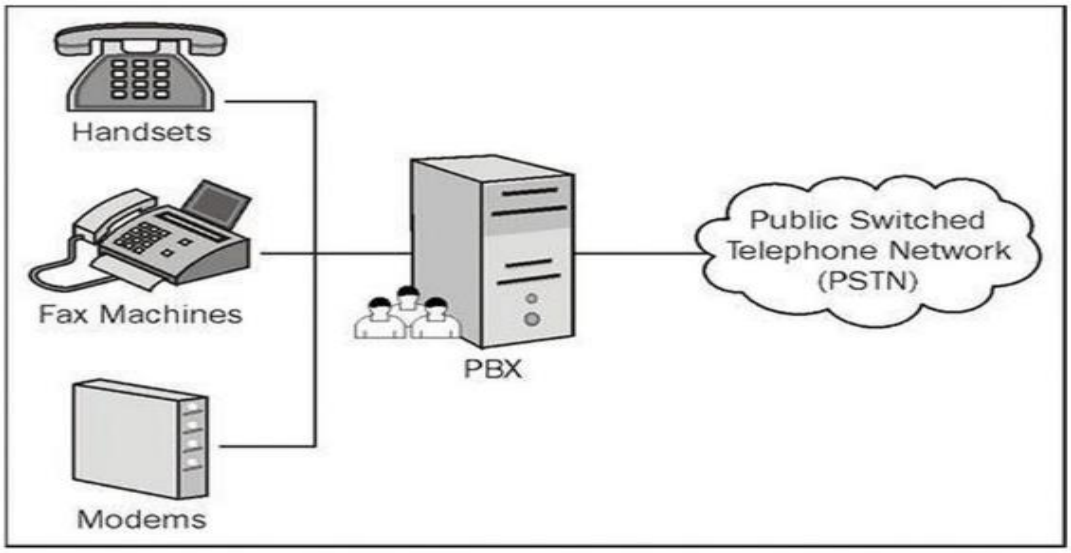


Figure III.2. Schéma descriptif d'appels d'extension à extension [19].

Chaque extension dans le schéma peut être directement connectée à une autre extension, sans passer par un système intermédiaire. Par exemple, un modem peut envoyer un fax à

Un télécopieur local en établissant une connexion directe entre les deux appareils via le PBX.

III.2.1.2. Regroupement des lignes

Une autre fonctionnalité offerte par Asterisk est le regroupement de lignes. Cette option permet de partager l'accès à plusieurs lignes téléphoniques. Ces lignes peuvent servir à se connecter au réseau téléphonique mondial, le Réseau Téléphonique Public Commuté (RTPC), ou être utilisées comme lignes privées pour d'autres systèmes téléphoniques. Le regroupement de lignes peut inclure une seule ligne analogique, plusieurs lignes analogiques ou des connexions numériques à haute capacité permettant de gérer plusieurs appels simultanés sur une seule connexion [19].

III.2.1.3. Fonctionnalités des opérations télécom

Asterisk offre un ensemble complet de fonctionnalités que l'on retrouve chez les opérateurs télécoms traditionnels. Il permet notamment l'identification de l'appelant, le routage des appels en fonction de cette identification, ainsi que d'autres services tels que l'appel en attente, le rappel d'appel (*69), la sonnerie distinctive, le transfert d'appels, le renvoi d'appel, et bien d'autres encore. Ces fonctionnalités de base et avancées sont prises en charge par Asterisk [19].

III.2.1.4. Distribution avancée des appels

Asterisk permet aux utilisateurs de recevoir et d'analyser les appels téléphoniques, en prenant des décisions basées sur les attributs de l'appel. Si le fournisseur de connexion du PSTN ne fournit pas suffisamment d'informations, les utilisateurs peuvent demander à l'appelant de les récupérer en utilisant un téléphone à écran tactile. L'Advanced Call Distribution (ACD) permet aux utilisateurs de servir efficacement les clients en utilisant des fichiers d'appel en attente. Asterisk ne nécessite pas de licence spéciale pour ACD, et le nombre d'appels peut être limité par le matériel utilisé [19].

III.2.1.5. Les enregistrements des détails d’appel

Les enregistrements de détails d'appel (CDR) sont stockés dans des bases de données ou des fichiers plats en utilisant Asterisk. Ils aident à surveiller l'utilisation du système Asterisk, à identifier les tendances et à comparer les documents avec les factures de l'entreprise Téléphonique. Ils évaluent l'activité des appels, identifient les numéros fréquemment appelés et ciblent les publicités. La durée de l'appel est également analysée [19]

III.2.1.6. Enregistrement des appels

Nous pouvons enregistrer les appels téléphoniques effectués via le PBX grâce à Asterisk, Ceci peut être utilisé pour fournir des matériels de formation et des exemples d'appels réussies et non réussis. En outre, le matériel d'appel peut être fourni à des partenaires ou des consommateurs, ce qui peut être utile dans un litige juridique. Il est crucial de tenir compte de cette fonctionnalité lors de la configuration de votre service Asterisk car, si votre PBX va gérer et enregistrer un nombre important d'appels, vous devrez peut-être résoudre de sérieuses difficultés matérielles et de stockage. Cette fonction est offerte par Asterisk; il nous appartient de décider si son utilisation dans une situation donnée est acceptable, légale et bénéfique [19].

III.2.1.7. Appel parking

Pour les utilisateurs encore habitués aux anciens systèmes de clés, le stationnement d'appel est une excellente fonctionnalité qui vous permet de prendre un appel, de le placer dans un emplacement de stationnement, puis de permettre à une autre personne au bureau de prendre cette ligne en accédant à l'emplacement. Ce processus imite l'ancienne approche du système de clés où vous prenez un appel, placez l'appelant en pause, puis communiquez le numéro de ligne à une autre personne au bureau. Au lieu d'un numéro de ligne, le parking d'appel donnera à un employé un numéro d'emplacement, qui, s'il est appelé, vous permettra de récupérer cet appel stationné. Le numéro de machine à sous sera communiqué à l'utilisateur en transférant l'appelant dans le parking d'appels, qui est accessible en appelant le code de caractéristique de stationnement [19].

III.2.1.8. Voicemail

Permet aux appelants de laisser des messages vocaux lorsqu'un utilisateur n'est pas disponible. Asterisk fournit un système de messagerie vocale robuste avec des fonctionnalités telles que la notification par courriel, voicemail-to-email et la transcription vocale-à-texte [20].

III.2.1.9. Messagerie unifiée

Intègre divers canaux de messagerie tels que le courrier vocal, l'e-mail, le télécopieur et les messages instantanés dans une seule boîte de réception pour un accès et une gestion unifiée [21].

III.2.1.10.VOIP Getway

Permet à Asterisk de se connecter et d'interagir avec les réseaux PSTN (Public Switched Téléphone Network) et VoIP traditionnels, en permettant des fonctionnalités telles que le

routage le moins coûteux et le pont d'appel [22].

III.2.2. Flexibilités et extensibilités d'Asterisk

Asterisk est conçu pour être un système de commutation de téléphonie (PBX) qui peut être étendu et personnalisé pour répondre aux besoins spécifiques d'une entreprise ou d'un réseau. Cette flexibilité est due à plusieurs facteurs :

III.2.2.1. Modularité

Asterisk est composé de plusieurs modules qui peuvent être ajoutées ou retirées en fonction des besoins. Chaque module est responsable d'une fonctionnalité spécifique, comme la gestion des appels, la messagerie vocale, ou la conférence. Cela permet aux utilisateurs de choisir les fonctionnalités qu'ils veulent utiliser et de les configurer indépendamment les unes des autres [23-25].

III.2.2.2. API de programmation

Asterisk offre une interface de programmation (API) qui permet aux développeurs de créer des applications personnalisées pour répondre aux besoins spécifiques de leur entreprise. Cela signifie que les utilisateurs peuvent créer des applications qui interagissent avec Asterisk pour offrir des fonctionnalités telles que la gestion des appels, la messagerie vocale, ou la conférence [23-25].

III.2.2.3. Support plusieurs protocoles

Asterisk peut être utilisé avec différents protocoles de téléphonie IP, tels que SIP, IAX et H.323. Cela offre aux utilisateurs la possibilité de sélectionner le protocole adapté à leur environnement et de le personnaliser pour répondre à leurs besoins particuliers [23-25].

III.2.2.4. Compatibilité avec d'autres systèmes

Il est possible d'intégrer Asterisk à d'autres systèmes, comme des systèmes de gestion de la chaîne d'approvisionnement, des systèmes de gestion de la production ou des systèmes de gestion de la relation client. Les utilisateurs ont la possibilité de concevoir des solutions de téléphonie IP qui s'intègrent à leurs processus métier particuliers [23-25].

III.2.3. Présentation des distributions et des forks bases sur Asterisk

III.2.3.1. FreePBX

C'est une GUI (interface utilisateur graphique) open source basée sur le Web qui contrôle et gère Asterisk (PBX), un serveur de voix sur IP. Il est aussi un outil de gestion d'astérisque basé uniquement sur le Web/php, où Asterisk est un logiciel. Ensemble, ces deux éléments constituent un système de communication complet pour la téléphonie Internet. Si nous avons examiné Asterisk, nous savons qu'il n'est livré avec aucune programmation « intégrée ». Nous ne pouvons pas y brancher un téléphone et le faire fonctionner sans modifier les fichiers de configuration, écrire des plans de numérotation et divers dérangements. Il est très facile avec l'interface graphique d'attribuer/supprimer des extensions, de configurer des lignes réseau, etc [27].

Figure III.3. Logo de FreePBX.

Quelques-unes des principales fonctionnalités de FreePBX sont les suivantes :

- Le plan de numérotation est configuré : Pour acheminer les appels entrants et sortants, FreePBX simplifie la configuration du plan de numérotation.
- Administration des utilisateurs et des extensions : Créer, modifier et supprimer des utilisateurs, des extensions et des services associés (messagerie vocale, file d'attente, etc.) est simple.
- Groupes d'appel nouveaux : Les files d'attente d'appels, les groupes de sonnerie et les menus vocaux interactifs (IVR) peuvent tous être configurés.
- Rapports et journaux : Les rapports détaillés sur les appels entrants, sortants, les files d'attente et l'utilisation des ressources sont fournis par FreePBX.
- Création de trunks VoIP : Capacité d'intégrer plusieurs trunks VoIP (SIP, IAX et DAHDI) pour la téléphonie sur IP.

III.2.3.2. Issabel

Issabel est un logiciel libre et open source qui unifie les communications dans une seule plate-forme. Il est basé sur Asterisk et intègre PBX, la messagerie, les tâches de collaboration et un serveur de base de données. La plate-forme vise à évoluer selon les besoins, en mettant l'accent sur une philosophie open-source et l'engagement de la communauté. La communauté Issabel regroupe des spécialistes du monde entier qui croient au pouvoir transformateur des technologies de l'information et de la communication. La structure du projet est modélisée sur Source Forge, avec le développement continu de nouveaux add-ons et versions pour répondre à divers besoins [29].

Figure III.4. Logo de Issabel.

- Vue d'ensemble de la fonctionnalité d'Issabel : Les appels vocaux, les vidéoconférences, les messages instantanés et la messagerie vocale ne sont que quelques-unes des fonctions de communication unifiées offertes par la plate-forme logicielle libre et open-source Isabel. En outre, une variété d'add-ons sont disponibles pour élargir ses capacités et satisfaire les exigences particulières de l'entreprise [29].

III.2.3.3. Elastix :

Elastix est un logiciel libre d'autocommutateur téléphonique privé (PBX) ou IPBX, basé sur le logiciel libre Asterisk. Elastix encapsule Asterisk et l'interface FreePBX dans une interface web globale de style Trixbox. Elastix est 100 % libre et sous licence GPLv2. Le CD Elastix (téléchargeable) inclut le noyau CentOS pour le système d'exploitation, Asterisk, pour la partie IPBX et interface web, et Flash Operator Panel (FOP) pour la partie graphique de l'interface web. Une fois le produit installé, l'administration de Elastix est entièrement réalisée depuis une interface web. Un accès SSH est parfois utile lors de l'ajout de nouveaux modules fonctionnels, comme les

modules de gestion de téléphone SIP de Astra Technologies [30].

Figure III.5. Logo d'Elastix

III.3. Systèmes de supervision

III.3.1. Définition

La supervision informatique, également connue sous le nom de monitoring informatique, consiste à collecter et analyser des données sur la performance, la disponibilité et la sécurité de votre système d'information. Ces données, provenant de diverses sources telles que serveurs, bases de données, applications et équipements réseau, permettent de créer une cartographie complète et en temps réel de votre infrastructure technologique [31].

III.3.2. Objectif

L'objectif de la supervision informatique est de détecter, diagnostiquer et résoudre de manière proactive les risques et incidents potentiels sur un système supervisé, afin d'éviter toute interruption de service [31].

III.3.3. Types

Il existe plusieurs types de supervision informatique essentiels pour gérer et maintenir efficacement votre infrastructure informatique. Comprendre ce qui doit être surveillé est crucial pour optimiser l'utilisation des ressources et du temps disponibles [31].

Voici quelques-uns des éléments les plus couramment supervisés :

III.3.3.1. Supervision des serveurs

Ce type de supervision contrôle les performances et la disponibilité des serveurs. Il surveille l'utilisation des ressources système telles que le processeur et la mémoire, et détecte les baisses de régime ou les défaillances matérielles afin de prévenir tout problème majeur [31].

III.3.3.2. Supervision du réseau

Cette supervision sonde les équipements réseau (routeurs, commutateurs, points d'accès sans fil) pour détecter les problèmes susceptibles d'affecter la bande passante ou la latence [31].

III.3.3.3. Supervision des applications

Elle fournit un aperçu détaillé des performances des applications, permettant d'identifier les services défaillants qui pourraient entraîner des problèmes critiques [31].

III.3.3.4. Supervision des bases de données

Elle suit l'évolution des bases de données et détecte les erreurs ou corruptions de données pouvant affecter la stabilité des systèmes [31].

III.3.4. Supervision de téléphonie mobile

Le concept de supervision dans la téléphonie IP consiste à surveiller en temps réel les lignes téléphoniques et les postes de travail pour garantir leur disponibilité et optimiser leur gestion. Cette supervision permet de visualiser l'état des lignes, qu'elles soient libres, en train de sonner, ou occupées, facilitant ainsi des décisions rapides et efficaces. Les avantages incluent un gain de temps en évitant les appels inutiles, une gestion simplifiée des transferts d'appels, et une aide à l'interception des appels en cas d'absence d'un collaborateur. En résumé, la supervision en téléphonie IP offre une vue d'ensemble de l'activité des collaborateurs, permet une gestion rapide et ergonomique des lignes téléphoniques, et améliore la communication interne et externe de l'entreprise [32, 33].

III.3.5. Composants des systèmes de supervision

III.3.5.1. Surveillance (Monitoring)

Collecte de Données en Temps Réel : Capture des métriques de performance et des états des équipements et des réseaux.

Analyse Continue **:** Utilisation de seuils prédéfinis pour détecter les anomalies et les problèmes potentiels.

Visualisation : Affichage des données en temps réel à travers des tableaux de bord et des graphiques.

III.3.5.2. Suivi (Tracking)

Historique des Performances : Enregistrement des données sur une période prolongée pour analyser les tendances et les comportements des systèmes.

Journalisation : Captures des événements et des actions pour un audit ultérieur et une traçabilité complète.

III.3.5.3. Pilotage (control)

Automatisation des Réactions : Mise en place de scripts et d'actions automatiques en réponse à certaines conditions (redémarrage de services, ajustements de configurations).

Gestion des Configurations : Contrôle centralisé et déploiement des configurations des équipements réseau et des serveurs.

III.3.5.4. Alertes

Notification en Temps Réel : Envoi d'alertes via divers canaux (emails, SMS, notifications push) en cas de détection de problèmes.

Priorisation des Alertes : Classification des alertes par niveaux de gravité pour une gestion efficace des incidents critiques en premier.

III.3.5.5. Rapports (reporting)

Rapports Réguliers : Génération de rapports périodiques sur les performances, les incidents et les interventions.

Analyse des Tendances : Utilisation des données historiques pour prévoir les besoins futurs et identifier les tendances récurrentes.

Conformité et Audit : Fourniture de documents pour les audits internes et externes, assurant la conformité aux normes et aux réglementations.

III.3.6. Outils et technologies de supervision

Les logiciels de supervision sont des solutions applicatives répondant au concept de supervision. Selon le mode de licence, on distingue deux types de logiciel de supervision :

III.3.6.1. Logiciels libres

i. CACTI

CACTI est un logiciel de surveillance qui fonctionne comme le front-end du RRDTool (graphical user interface). Il est basé sur un serveur Web qui utilise PHP et une base de données MySQL. RRDTool permet de créer des graphiques et de stocker toutes les données de surveillance réseau. Ces détails sont récupérés via SNMP et MRTG.

Ainsi, CACTI permet la représentation graphique de divers états périphériques réseau en utilisant SNMP ou même des scripts (Bash, PHP, Perl, VBs, etc.) pour avoir, par exemple, l'espace disque restant ou la mémoire utilisée, la charge du processeur ou Ping d'un élément actif [34].

Figure III.6. Logo de CACTI

Cet élément n'est pas un outil de supervision au sens strict du terme et il n'a pas la capacité de recevoir des traps [35].

- Avantages :
  - L'installation est simple et directe.
  - La configuration est facile à réaliser.
  - Il offre un affichage rapide des graphiques sur diverses périodes.
  - Il peut être amélioré grâce à l'ajout de plugins.

Il bénéficie d'une large communauté de soutien.

- Inconvénients :
  - Les fonctionnalités de base peuvent être limitées.
  - La génération des graphiques peut prendre un certain temps.

ii. ZABBIX

Zabbix a été fondé par Alexe iVladishev et est actuellement activement développé et entretenu par ZABBIX SIA. Zabbix est une plateforme d'alerte et de surveillance gratuite en temps réel. La supervision de l'ensemble des équipements réseautiques est son

principal mais. Elle peut, cependant, surveiller les changements de température, d'humidité, de tension électrique et d'autres mesures qui ne sont pas spécifiquement liées aux environnements informatiques. Ce logiciel libre surveille presque tous les composants du réseau ainsi que l'intégrité et la santé des serveurs [34].

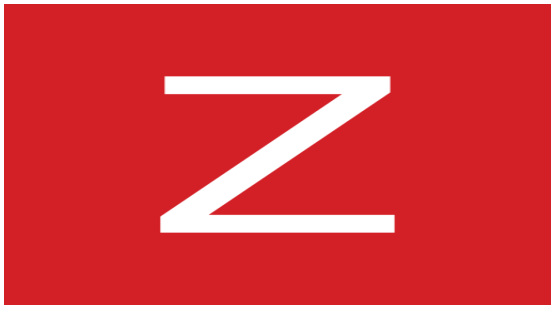


Figure III.7. Logo de Zabbix

- Caractéristiques :
  - Il s'agit d'un outil de supervision.
  - Il est capable de découvrir automatiquement les machines sur le réseau.
  - Il permet l'implémentation de tests indépendants sur les machines.
  - Il gère les alertes.
- Avantages :
  - L'installation est simple et sans tracas.
  - Il permet une génération aisée de graphiques.
  - Il offre une consultation facile des graphiques en fonction du temps.

Les erreurs sont clairement affichées sur le tableau de bord.

- Inconvénients :
  - Chaque machine à surveiller doit être équipée du client Zabbix.
  - Sans le client, les fonctionnalités sont limitées au ping.
  - Il y a un risque de surcharge d'alertes.
  - Il manque de flexibilité dans certaines situations.

iii. NAGIOS

Nagios est un logiciel de surveillance gratuit disponible sous la GPL qui permet de surveiller le réseau et le système. En outre, il surveille les hôtes et les services désignés, en informant les utilisateurs quand des dysfonctionnements du système se produisent et

quand le fonctionnement normal du système reprend.

NAGIOS récupère les données fournies par les services de surveillance et d'analyse. Si les résultats de l'analyse indiquent un problème, les services de surveillance ont la possibilité de notifier l'administrateur réseau via une variété de canaux, y compris les SMS, les messages instantanés, le courrier électronique, et plus encore [31].

Figure III.8. Logo de Nagios

- Caractéristiques :
  - Le superviseur chargé de superviser les tâches de surveillance
  - Une interface web
  - Plugins
  - Une architecture qui est Master/Slave
- Fonctionnalités :
  - Le suivi des services tels que SMTP, POP3, HTTP, FTP, etc.
  - Le contrôle des ressources d'un ordinateur, comme la charge du processeur et l'espace disque.
  - La capacité à créer ses propres plugins.
  - L'organisation hiérarchique des dispositifs qui composent le réseau.
  - L'envoi de notifications par email.
  - L'enregistrement des événements.

De plus, Nagios peut opérer en deux modes : en utilisant une base de données ou en mode texte.

- Avantages [35] :
  - Grosse communauté et bonne réputation
  - Extrêmement robuste et polyvalente
  - Capable d'avoir une surcouche de graphène (Centreon) : fournit la gestion du graphène.
  - Capable d'utiliser une variété de plugins
- Inconvénients [35] :
  - Il est difficile à installer et à configurer.
  - Nagios a une interface ouverte
  - Nagios ne permet pas d'ajouter des hosts via Web

III.3.6.2. Logiciels propriétaires

- IBM Tivoli Netview : Ce logiciel est le résultat de l'acquisition par IBM de la société Tivoli. C'est l'un des logiciels commerciaux les plus utilisés. Il s'agit d'un groupe de logiciels, dont l'un est Tivoli Monitoring, qui est principalement utilisé pour la surveillance de machines ou d'applications [34].
- HP Open View : Une solution de surveillance modulaire très complète développée par HP. Globalement, il permet de cartographier automatiquement et dynamiquement le réseau, de recueillir des informations de surveillance, de les corréler, d'envoyer des alertes, de maintenir une base de données simplifiée pour l'analyse de l'historique des événements et, en fin de compte, de produire des rapports basés sur des graphiques [34].
- Big Brother : Superviseur de services de base qui fonctionne sous Windows NT. Il est efficace mais ne peut superviser qu'un petit nombre de services tels que HTTP, POP, NNTP et SMTP. De plus, il n'est pas possible d'ajouter de nouvelles fonctionnalités et il n'est pas possible de remonter les alarmes autrement que graphiquement [34].
- Cisco Works 2000 : Outil de supervision propriétaire Cisco idéal pour la surveillance et la configuration du matériel Cisco. De plus, il facilite la configuration graphique du matériel

III.4. Conclusion

Ce chapitre a exploré en détail Asterisk Systems, une plate-forme IPBX open source qui offre de nombreuses fonctionnalités pour connecter des réseaux vocaux, ainsi que diverses distributions et forks Asterisk tels que FreePBX, Issabel et Elastix.

Nous avons également présenté les concepts et composants de base des systèmes de gestion informatique qui sont essentiels pour maintenir la disponibilité et la performance des infrastructures technologiques.

Parmi les différents outils de surveillance présentés, tant gratuits que propriétaires, Nagios a été choisi comme solution d'implémentation. Bien que l'installation et la configuration initiales présentent des difficultés, Nagios propose une solution robuste et polyvalente qui bénéficie d'une large base d'utilisateurs.

En mettant en œuvre un système de surveillance comme Nagios, nous pouvons surveiller de manière proactive l'état de notre infrastructure, identifier rapidement les pannes potentielles grâce à un système d'alerte en temps réel et créer des rapports détaillés. Cette visibilité accrue de nos systèmes nous permet d’assurer une disponibilité maximale de nos services et une expérience utilisateur optimisée.

Chapitre IV
Réalisation et Test

IV.1. Introduction

Après avoir passé en revue le choix de la solution de supervision dans le chapitre précédent, nous procédons dans ce chapitre à la réalisation d'un environnement VoIP virtuel, principalement à l'aide d'un simulateur ***Oracle VirtualBox***. Nous mettrons en place un serveur de supervision basé sur une solution open source (***Nagios***) avec deux autres serveurs VoIP, ***FreePBX*** et ***Issabel***. Ensuite, nous développerons des scripts pour que ces serveurs transmettent l'état de leurs services téléphoniques au serveur de supervision via son interface web en temps réel. Enfin, cette solution doit permettre d'envoyer des alertes en cas de panne.

IV.2. Présentation et implémentation de solution

Notre travail consiste à mettre en place un système de communication basé sur VoIP.

IV.2.1. Installation des périphériques

Simulateur **:** Oracle VirtualBox

Logiciels utilisés :

- *FreePBX*,
- *Issabel*,
- *Nagios*,
- *hMailServer*,
- *Thunderbird*.

Softphones : sont des logiciels installés sur les ordinateurs et qui assure toutes les fonctions téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC on 'a choisissait :

- *MicroSip*
- *Zoiper*

IV.2.2. Implémentation de la solution

Premièrement, nous allons mettre en place une machine virtuelle ***Oracle VirtualBox*** dans laquelle nous installerons.

- Les deux distributions open source de la téléphonie IP : *FreePBX* et *Issabel*
- Le serveur de supervision *Nagios*

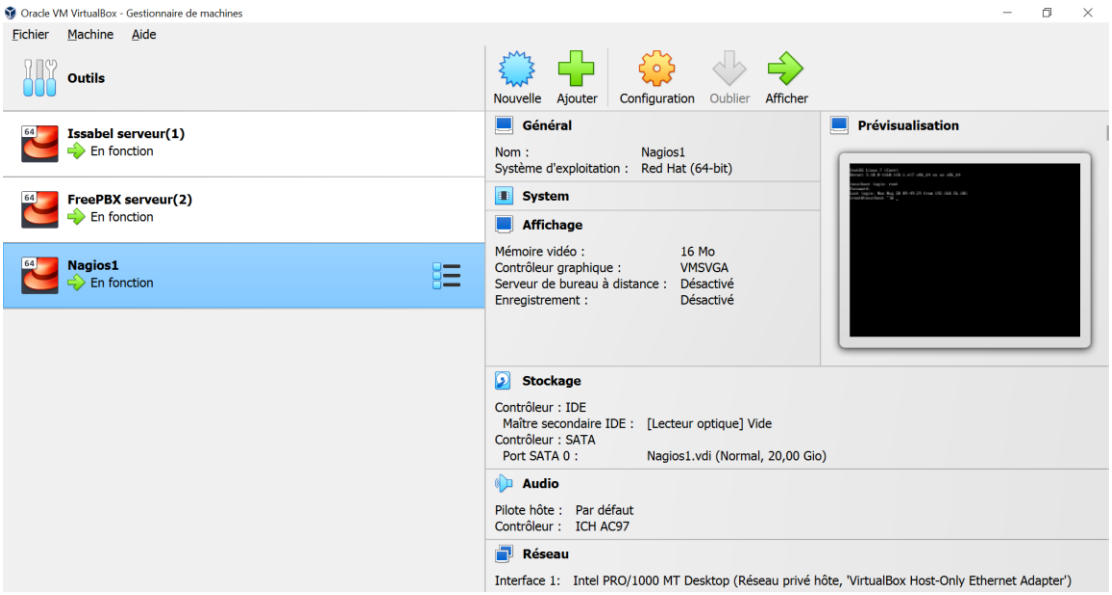


Figure IV.1. Implémentation des serveurs sur VirtualBox

En second lieu, nous allons effectuer une configuration basique nécessaire à l'établissement d'un appel entre nos deux serveurs *FreePBX* et *Issabel* :

D'abord, nous créerons deux extensions sur le premier serveur *FreePBX* (4000 et 4001) et deux autres sur le deuxième serveur *Issabel* (3000 et 3001).

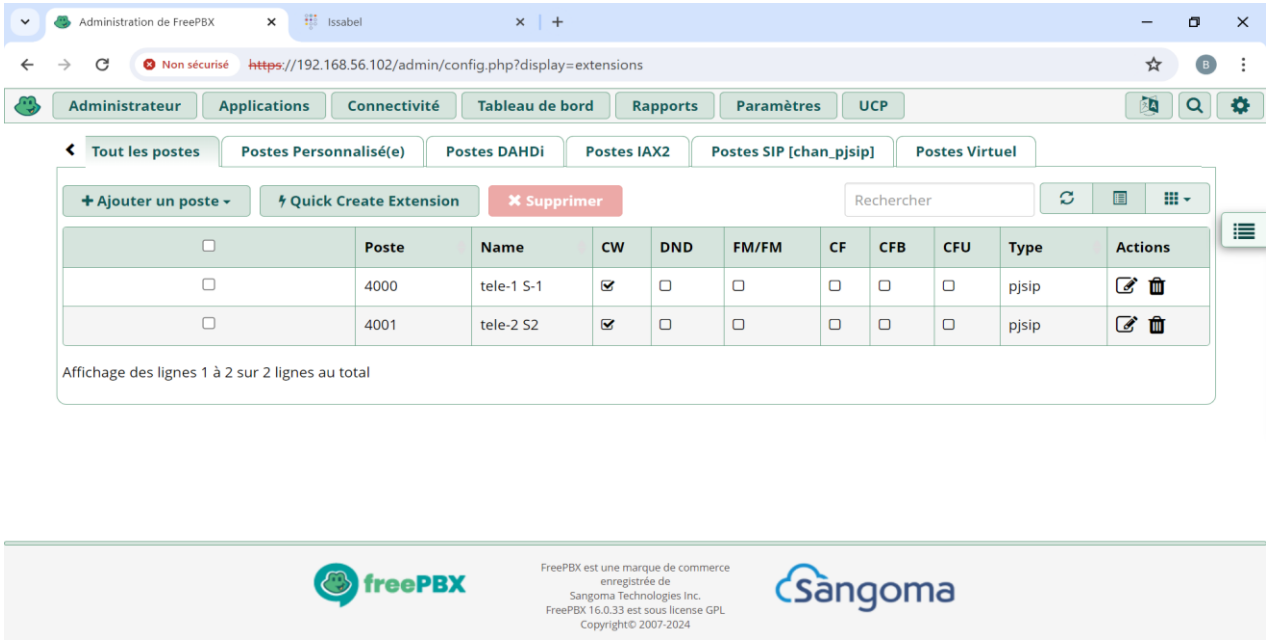


Figure IV.2. Extensions crées sur le serveur FreePBX

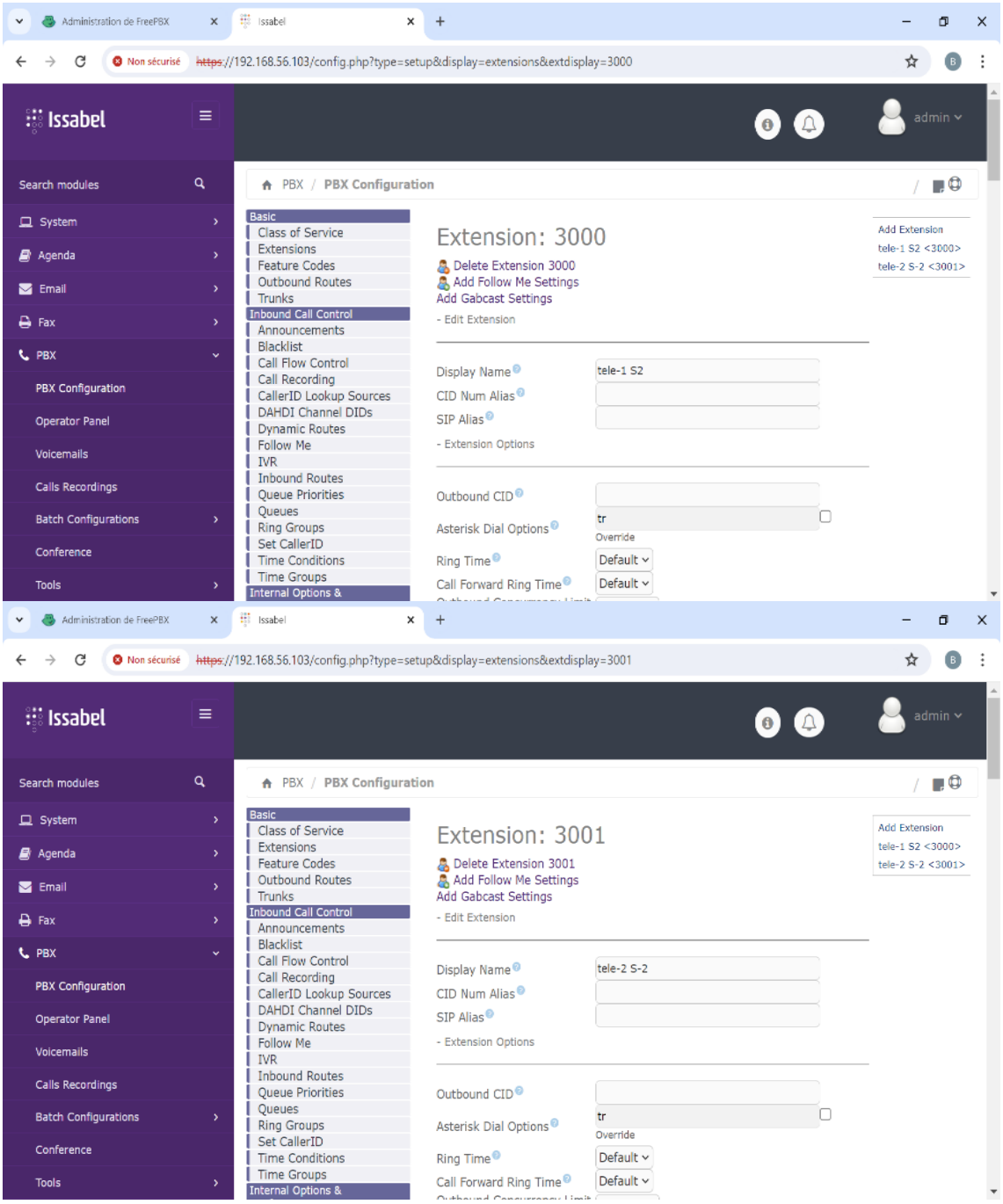


Figure IV.3. Extensions crées sur le serveur Issabel

Ensuite, nous allons installer et configurer deux softphones sur Windows :

***MicroSip* :** est un softphone SIP portable disponible pour Microsoft Windows. Il facilite les appels VoIP de haute qualité basée sur le protocole SIP ouvert. *MicroSIP* appartient à la catégorie des logiciels gratuits et open source.

Figure IV.4. Microsip

- ***Zoiper :*** est une solution de numérotation softphone multi-plateforme VoIP qui prend en charge les appels vocaux et vidéo ainsi que la fonctionnalité de messagerie instantanée. Disponible pour Windows, Mac et Linux.

Figure IV.5. Zoiper

- Dans notre premier softphone *MicroSip*, nous créerons deux comptes : unpour le serveur *FreePBX* (4000) et l'autre pour le serveur *Issabel* (3000).

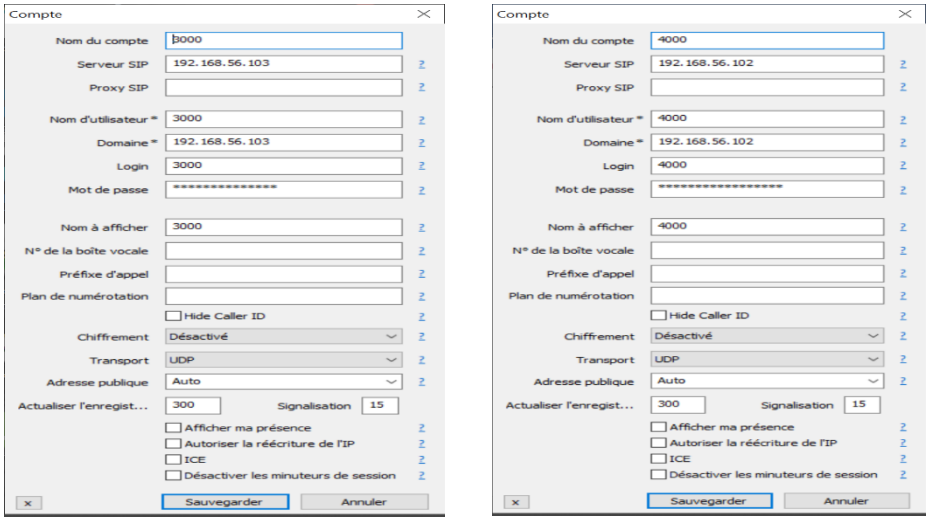


Figure IV.6. Configuration du compte MicroSIP

- Dans le deuxième softphone *Zoiper*, nous créerons également deux comptes : un pour le serveur *FreePBX* (4001) et l'autre pour le serveur *Issabel* (3001).

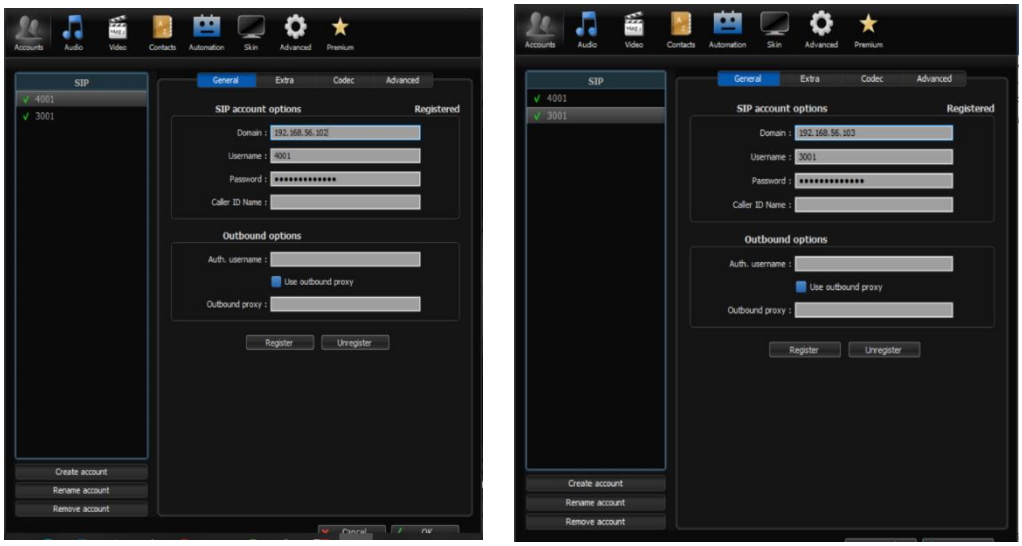
- 

Figure IV.7. Configuration du compte Zoiper

Actuellement, les appels passent entre les deux softphones du même serveur mais ne passent pas entre les contacts qui ne sont pas sur le même serveur.

Figure IV.8. Test d'appel sur le serveur Issabel

Figure IV.9. Test d'appel sur le serveur FreePBX

- Maintenant, nous allons configurer le trunk et le routage entre les deux serveurs pour permettre les appels entre tous les contacts.

Figure IV.10. Test d'appel entre les deux serveurs

IV.3. Configuration de la solution

Dans cette étape, nous allons configurer notre serveur de supervision *Nagios* en commençant par la création des hôtes, suivie de la configuration des services.

IV.3.1. Création des hôtes

Etape 1 : Création du fichier de configuration des hôtes

Tout d'abord, nous allons créer un script nommé script.cfg dans *Nagios*. Dans ce script, nous ajouterons chaque serveur VoIP (*FreePBX* et *Issabel*) en tant qu'hôte. Ensuite, nous ajoutons les définitions des hôtes pour chaque serveur VoIP :

Figure IV.11. Définir des hôtes sur l'interface du Nagios

Nous allons définir les paramètres de base pour chaque hôte, tels que l'adresse IP, le nom d'hôte et le groupe d'hôtes auquel il appartient.

Etape 2 : Déclaration du fichier de configuration dans Nagios

Nous déclarerons ce script comme fichier de configuration dans Nagios en ajoutant la ligne suivante au fichier de configuration principal de *Nagios.*

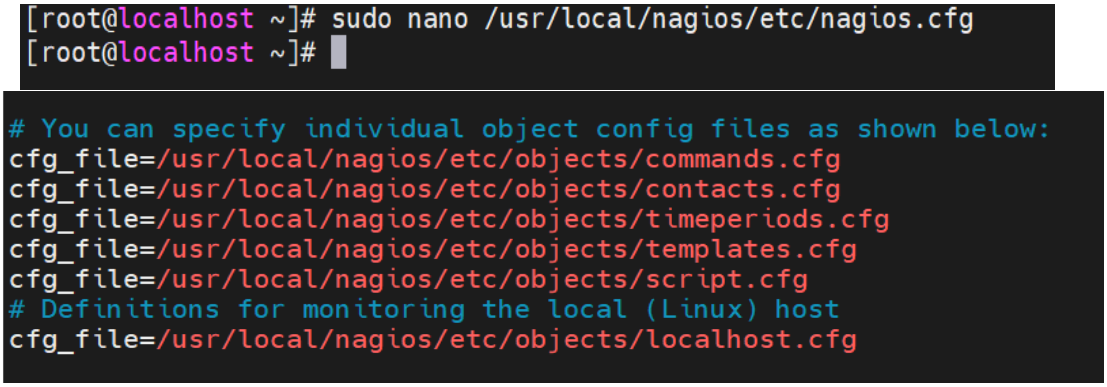


Figure IV.12. Déclaration du fichier de configuration des hôtes dans Nagios

Étape 3 : Vérification de la configuration

Après avoir configuré et revendiqué les hôtes, nous devons vérifier que Nagios reconnaît ces nouveaux hôtes. Pour ce faire, nous redémarrons le service Nagios et vérifions l'interface web.

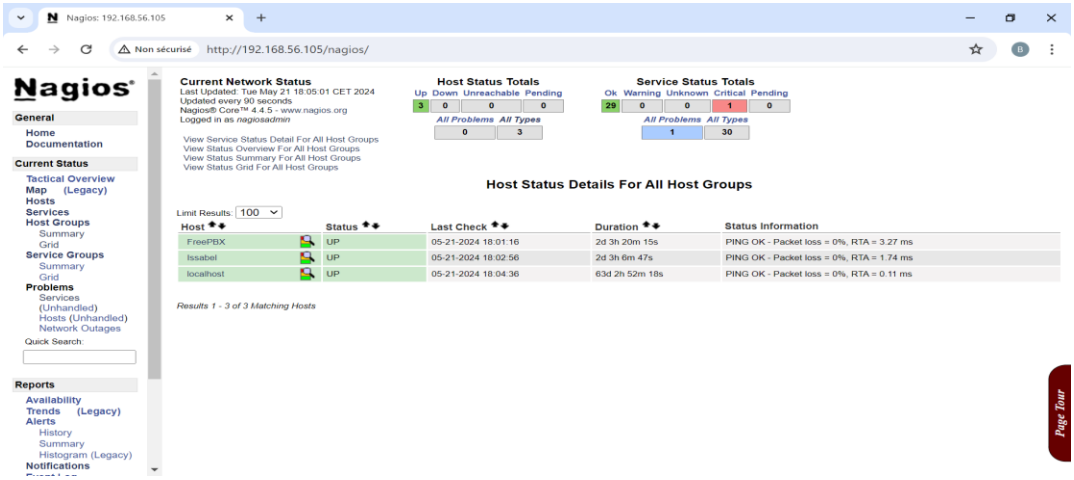


Figure IV.13. Interface web Nagios montrant les hôtes configurés

IV.3.2. Configuration des services

Cette étape consiste à déterminer les services spécifiques à surveiller pour chaque hôte, tels que la disponibilité des extensions, l'état des services web, le CPU, la ROM, la RAM et d'autres services. Nous allons procéder comme suit :

Étape 1 : Création des scripts

Tout d'abord, nous avons nommé le répertoire des scripts custom_scripts et créé les scripts requis pour la surveillance. Ensuite, nous allons créer les scripts nécessaires pour la surveillance

```
[root@localhost ~]# cd /usr/local/nagios/libexec/custom_scripts
[root@localhost custom_scripts]# ls
check_A_calls.sh         check_cpu.sh   check_Dphonees.sh  check_IP.sh   check_ROM.sh    check_Uphonees.sh
check_asteriskStatus.sh  check_Date.sh  check_hostname.sh  check_RAM.sh  check_trunk.sh
[root@localhost custom_scripts]#
```

Figure IV.14. Création des scripts nécessaires

Remarque : chaque script on 'a rendu exécutable par la commande **<chmod +x check_*.sh>**

- Voici un exemple de contenu pour l'un des scripts, par exemple **check_cpu.sh**

```
#!/bin/bash
ipADDR=$1
warning=$2
critical=$3
# Exécute la requête SQL et stocke le résultat dans la variable 'query'
query=$(mysql -u root -proot -D nagios_db -e "SELECT cpu FROM Free_pbx_data WHERE ip='$ipADDR' ORDER BY id DESC LIMIT 1" | grep '[0-9]')
# Affiche le résultat de la requête SQL
value=$(echo "$query" | grep -o '[0-9]*')
echo "CPU: $value%"
# Vérifie si la valeur est vide ou non numérique
if [ -z "$value" ] || ! [[ "$value" =~ ^[0-9]+$ ]]; then
    echo "UNKNOWN: Aucune valeur numérique trouvée ou valeur non numérique"
    exit 3
fi
# Vérifie les seuils
if [ -n "$warning" ] && [ -n "$critical" ]; then
    if (( $(echo "$value <= $warning" | bc -l) )); then
        echo "OK : $value% CPU usage"
        exit 0
    elif (( $(echo "$value > $warning && $value < $critical" | bc -l) )); then
        echo "warning: $value% CPU usage"
        exit 1
    elif (( $(echo "$value >= $critical" | bc -l) )); then
        echo "critical: $value% CPU usage"
        exit 2
    else
        echo "UNKNOWN: Valeur inattendue"
        exit 3
    fi
else
    echo "UNKNOWN: Seuils non spécifiés"
    exit 3
-- INSERT --                                                    1,12          Top
```

Figure IV.15. Check_cpu.sh

Étape 2 : Intégration des scripts dans Nagios

Après avoir créé les scripts, nous les intégrerons dans la configuration Nagios en ajoutant les commandes correspondantes dans le fichier de configuration.

Dans le fichier de configuration des commandes Nagios nous Ajouter les définitions des commandes pour chaque script.

Exemple de script **check_cpu.sh :**

```
define command {

    command_name    check_cpu
    command_line    /usr/local/nagios/libexec/custom_scripts/check_cpu.sh $HOSTADDRESS$ $ARG1$ $ARG1$
}
```

Figure IV.16. Définir la commande pour check_cpu.

Étape 3 : Configuration des services dans Nagios

Enfin, nous avons définir les services à surveiller pour chaque hôte en utilisant les commandes que nous venons de créer. Pour chaque service, nous avons également défini des seuils pour les états "WARNING" et "CRITICAL".

Exemple de script check_cpu.sh

```
define service {
    use                     generic-service
    host_name               FreePBX
    service_description     Check_cpu
    check_command           check_cpu!80!90
}

define service {
    use                     generic-service
    host_name               Issabel
    service_description     Check_cpu
    check_command           check_cpu!80!90
}
```

Figure IV.17. Définir le service check_cpu

On redémarre notre serveur Nagios et vérifier sur son interface web s'il appliquer les changements. Maintenant, Nagios est configuré pour surveiller les services spécifiques de chaque hôte.

IV.3.3. Configuration des serveurs

Maintenant, notre étape consiste à relier nos serveurs. Nous commencerons par créer une base de données sur *Nagios*, suivie de l'étape de configuration SSH entre *Nagios* et *FreePBX*, ainsi qu'entre *Nagios* et *Issabel*.

IV.3.3.1. Création d'une base de donnée

Étape 1 : Création d'un utilisateur sur MySQL

Nous avons connecté à MySQL en tant que root et créez un utilisateur nommé user1, puis on 'a créé notre base de données personnelle nagios_db.

```
MariaDB [nagios_db]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| nagios_db          |
| performance_schema |
| test               |
+--------------------+
5 rows in set (0.00 sec)
```

Figure IV.18. Création de nagios_db

Étape 2 : Création d'une table pour les données

Dans cette étape, nous avons créé une table nommée **Serveurs_data** pour les deux serveurs *FreePBX* et *Issabel*, qui contiendra les services que nous voulons surveiller de façon dynamique.

```
MariaDB [nagios_db]> SHOW TABLES;
+---------------------+
| Tables_in_nagios_db |
+---------------------+
| Serveurs_data       |
+---------------------+
1 row in set (0.00 sec)

MariaDB [nagios_db]>
```

Figure IV.19. Création du Serveur_data

Remarque : après cette étape, nous avons inséré dans chaque script une commande qui permet d'obtenir les données qui sont insérer dans notre table de données :

```
# Exécute la requête SQL et stocke le résultat dans la variable 'query'
query=$(mysql -u root -proot -D nagios_db -e "SELECT cpu FROM Serveurs_data WHERE ip='$ipADDR' ORDER BY id DESC LIMIT 1" | grep '[0-9]')
```

Figure IV.20. Commande d'exécution

Étape 3 : Script de mise à jour des services

Sur chaque serveur de téléphonie IP (*FreePBX* et *Issabel*), nous avons créé un script nommé nagiosScript.sh qui contient tous les services et recueille les informations de chaque service de manière dynamique, puis les insère dans notre base de données *nagios_db*.

Dans chaque script, nous avons spécifié l'adresse IP de Nagios, le mot de passe de la base de données, et le nom de table.

IV.3.3.2. Configuration SSH

Pour permettre une communication sécurisée entre le serveur de supervision Nagios et les serveurs VoIP, nous configurons des connexions SSH. Cela implique de générer des clés SSH sur le serveur *Nagios* et de les copier sur les serveurs *FreePBX* et *Issabel*. Une fois cette configuration terminée, les serveurs peuvent échanger des données de manière sécurisée et automatisée.

```
[root@freepbx ~]# sh nagiosScript.sh
root@192.168.56.105's password:
[root@freepbx ~]#
```

Figure IV.21. Connexion SSH entre Nagios et FreePBX

IV.3.4. Notification par Email

L'envoi d'alertes par email est une étape cruciale dans la mise en place d'un système de supervision efficace. Ce processus permet aux administrateurs système de recevoir des notifications en temps réel si des anomalies ou des problèmes critiques sont détectés sur les serveurs surveillés. Voici les étapes pour configurer l'envoi d'alertes email à l'aide de *Nagios* et *hMailServer* :

- **Installation et Configuration de hMailServer**

Nous avons installé *hMailServer*, un serveur de messagerie open source. Sur *hMailServer*, nous avons défini un domaine et créé des comptes de messagerie pour les alertes *Nagios* (ibti@server.com et raf@server.com). Nous nous sommes assurés que le serveur de messagerie est capable d'envoyer des emails à la fois vers des adresses internes et externes. Pour cela, nous avons également installé le logiciel Thunderbird afin de pouvoir lire les messages reçus.

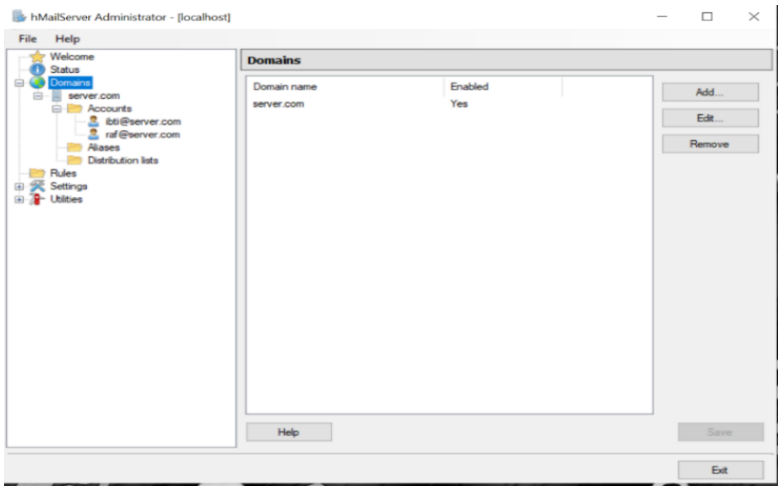


Figure IV.22. Interface de serveur hMail

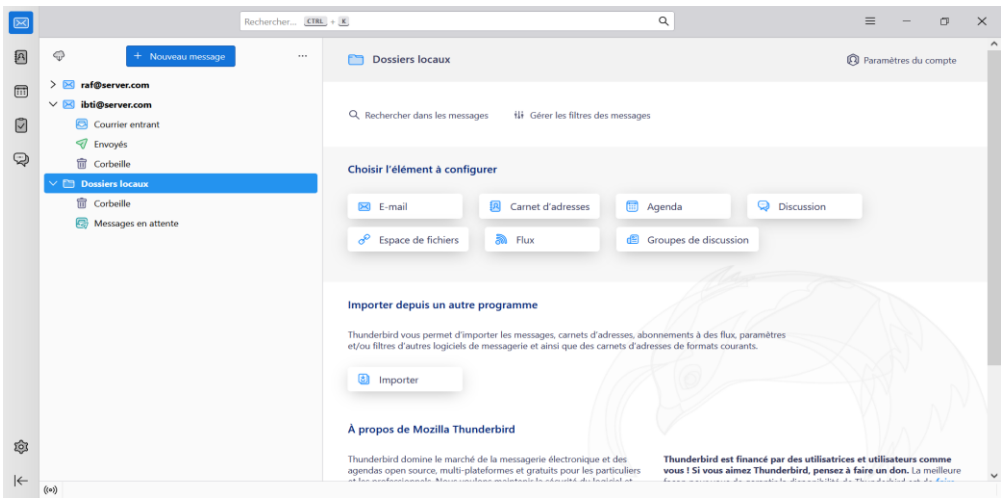


Figure IV.23. Interface de logiciel Thunderbird

- **Configuration de Nagios pour l'Envoi d'Alertes**

Étape 1 : Installation et Configuration de Postfix

On va utiliser *Postfix* est un serveur de messagerie SMTP populaire sur les systèmes Linux

Postfix doit être installé et correctement configuré pour fonctionner comme serveur de messagerie SMTP.

Après l'installation, on va modifier le fichier principal de configuration du *postfix* « main.cf» en ajoutant les paramètres nécessaires :

- Le nom de notre hôte « localhost.localdomain ».
- Notre domaine « localhost.localdomain ».
- L'adresse du serveur SMTP de notre réseau c'est la passerelle SMTP
- Notre destination locale ou bien extérieur.

Ensuit on va configurer *postfix* pour qu'il marche avec une authentification pour permettre à notre serveur d'envoyer des e-mails via un relais SMTP sécurisé.

On va utiliser une authentification SASL. Après avoir installé et configuré *Postfix*, nous devons créer un fichier pour stocker les informations d'identification SASL. « sudo nano /etc/postfix/sasl_passwd ».

Étape 2 : Configuration des Contacts dans Nagios

Dans Nagios, la configuration des contacts permet de définir les personnes ou les groupes qui recevront les notifications d'alertes.

Pour cela on va modifier le fichier « contacts.cfg » on va définir nos contacts qu'on a créé sur hmailserver. ibti@server.com , raf@derver.com

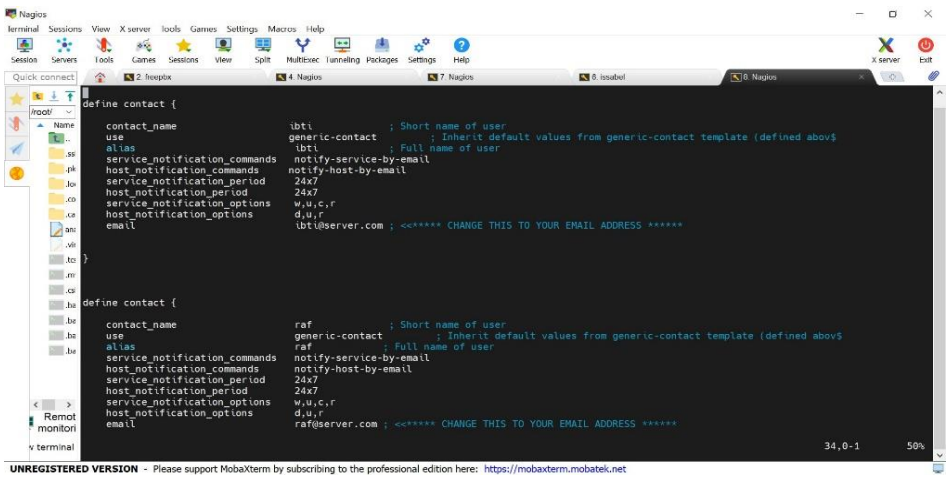


Figure IV.24. Définitions des contacts sur Nagios

On a fait aussi définir groupe des contacts, Les groupes de contacts permettent de regrouper plusieurs contacts. Cela facilite l'envoi de notifications à plusieurs personnes en même temps.

Étape 3 : Affectation des Notifications aux hôtes et services

On va affecter à chaque hôte et service les contacts qu'on a défini sur fichier du contact.

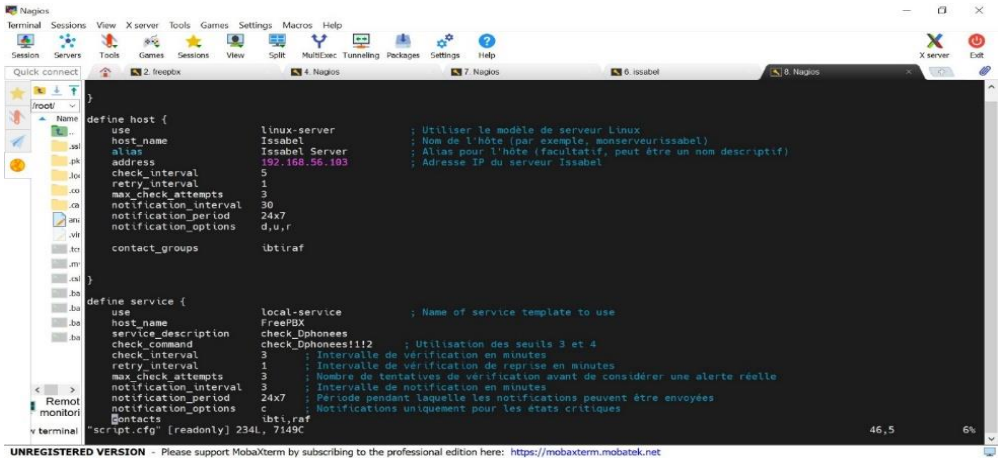


Figure IV.25. Affectations des contactes

On peut ajouter les Conditions de Vérification des Services comme :

- check_command : Détermine la commande et les seuils utilisés pour les vérifications.
- check_interval : Intervalle en minutes entre les vérifications régulières.
- retry_interval : Intervalle en minutes entre les vérifications en cas de problème détecté.
- max_check_attempts : Nombre maximum de tentatives de vérification avant de déclencher une alerte.
- notification_interval : Intervalle en minutes entre les notifications répétées.
- notification_period : Période pendant laquelle les notifications sont envoyées.
- notification_options : Types de notifications à envoyer (w = warning, u = unknown, c=critical, r = recovery).

Étape 4 : Définir les Commandes de Notification

On va Configurer les commandes que *Nagios* utilisera pour envoyer des notifications par e-mail en ajoutant sur le fichier « commands.cfg » les commandes de notification suivante :

- Commande pour les notifications des hôtes. « notify-host-by-email »
- Commande pour les notifications des services. « notify-service-by-email »

IV.4. Test de fonctionnement

IV.4.1. Supervision des serveurs téléphoniques

Dans cette étape, nous allons superviser nos hôtes que nous avons déjà ajoutés à notre serveur *Nagios*. Nous allons effectuer un test pour les deux hôtes, *FreePBX* et *Issabel*.

Nous allons éteindre notre serveur *Issabel* et laisser *FreePBX* en fonctionnement.

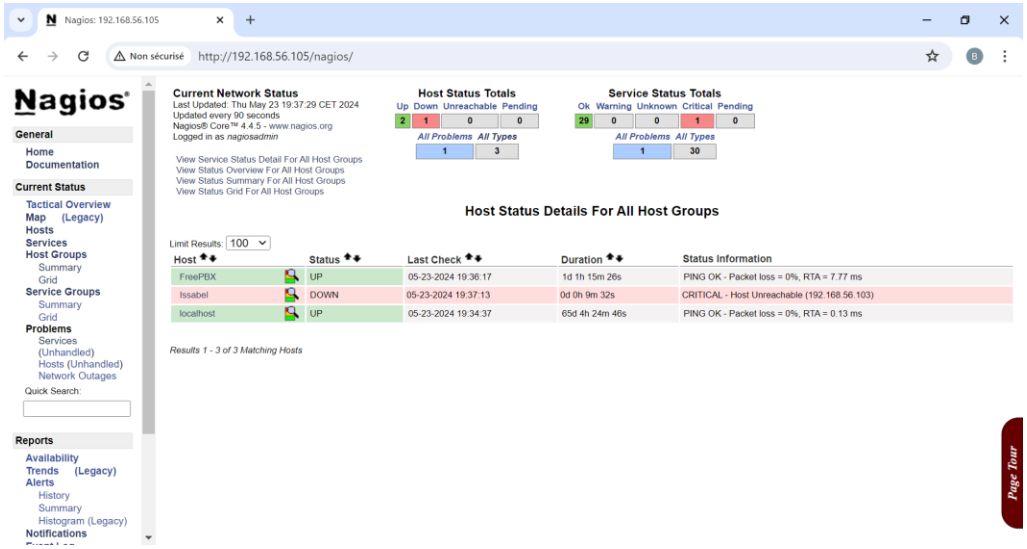


Figure IV.26. Test des hôtes sur l'interface Nagios

Remarque : Nous remarquons que notre serveur *Nagios* affiche "down" pour *Issabel* et "up" pour *FreePBX*, indiquant que notre première supervision fonctionne correctement.

IV.4.2. Supervision des services des serveurs

Dans cette partie, nous allons vous montrer comment notre **serveur** *Nagios* surveille les services de notre serveur configuré (CPU, RAM, ROM).

- Supervision de Cpu

Dans cette étape, nous allons tester notre CPU. Comme nous avons déjà défini les seuils de CPU dans Nagios, les états du CPU sont surveillés de la manière suivante :

Si la valeur du processeur est inférieure à 80 %, l'état de notre processeur affichera "OK" et sera vert.

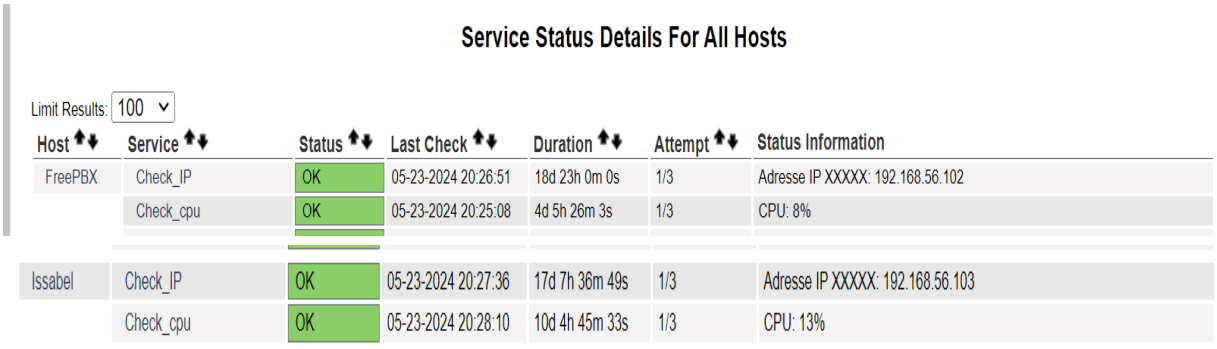


Figure IV.27. Test de Cpu des deux serveurs l'état « Ok ».

Si la valeur du CPU est supérieure ou égale à 80% mais inférieure à 90%, le statut affiche "WARNING" avec une couleur jaune.

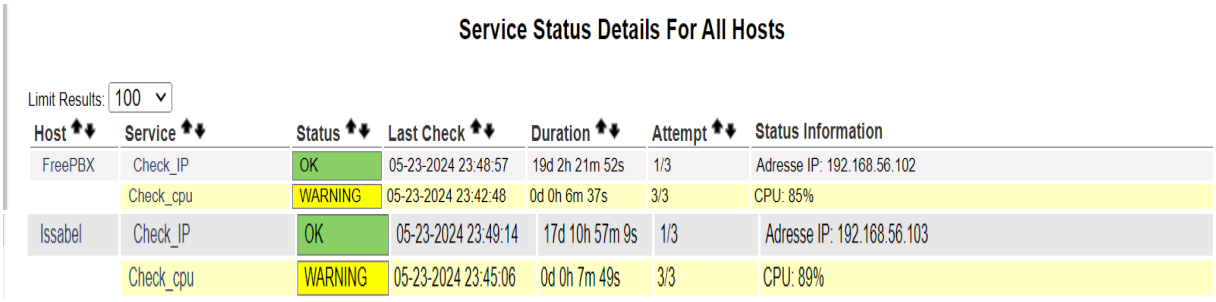


Figure IV.28. Test de Cpu des deux serveurs l'état « WARNING ».

Si la valeur du CPU est égale ou supérieure à 90 %, l'état affichera "CRITICAL" en rouge.

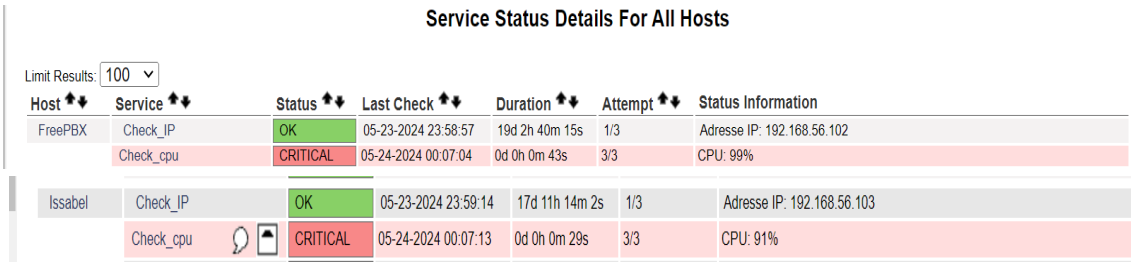


Figure IV.29. Test de Cpu des deux serveurs l'état « Critical ».

Remarque : Pour ce qui est de la supervision de la ROM et de la RAM, le principe est similaire à celui du CPU. Nous avons personnalisé les seuils en fonction de nos besoins, et le même protocole s'applique.

IV.4.3. Supervision des services téléphoniques

Dans cette étape de supervision des services téléphoniques, nous nous concentrons sur trois aspects principaux : les trunks, les téléphones actifs (up phones) et les téléphones inactifs (down phones).

IV.4.3.1. Supervision de Trunk

Les trunks jouent un rôle crucial dans la connectivité des appels téléphoniques en reliant différents réseaux de communication. La supervision des trunks implique de surveiller leur disponibilité, leur capacité à traiter les appels et leur qualité de service.

On 'a configuré déjà un trunk 'To-issabel' et un autre 'To-Freepbx' pour que les appelles passe entre les serveurs.

```
Endpoint:  4000/4000                                        Not in use    0 of inf
    InAuth:  4000-auth/4000
       Aor:  4000                                           1
     Contact:  4000/sip:4000@192.168.56.101:57670;ob      bedce15421 Avail        2.525

Endpoint:  4001/4001                                        Not in use    0 of inf
    InAuth:  4001-auth/4001
       Aor:  4001                                           1
     Contact:  4001/sip:4001@192.168.56.101:44679;rinstan e892e94493 Avail       40.365

Endpoint:  To-Issabel                                       Not in use    0 of inf
       Aor:  To-Issabel                                     0
     Contact:  To-Issabel/sip:192.168.56.103              c58a2f339e Avail        4.283
 Transport:  0.0.0.0-udp              udp      3     96  0.0.0.0:5060
  Identify:  To-Issabel/To-Issabel
      Match: 192.168.56.103/32
```

Figure IV.30. Configuration du trunk « to Issabel »

```
[root@issabel ~]# asterisk -rx 'sip show peers'
Name/username             Host                                  Dyn Forcerport Comedia    ACL Port     Status      Description

3000/3000                 (Unspecified)                          D  No         No          A  0        UNKNOWN

3001/3001                 192.168.56.101                         D  No         No          A  44679    OK (27 ms)

To-frpbx                  192.168.56.102                            Auto (No)  No             5060     OK (2 ms)
```

Figure IV.31. Configuration trunk « to FreePBX »

Sur interface **Nagios:**

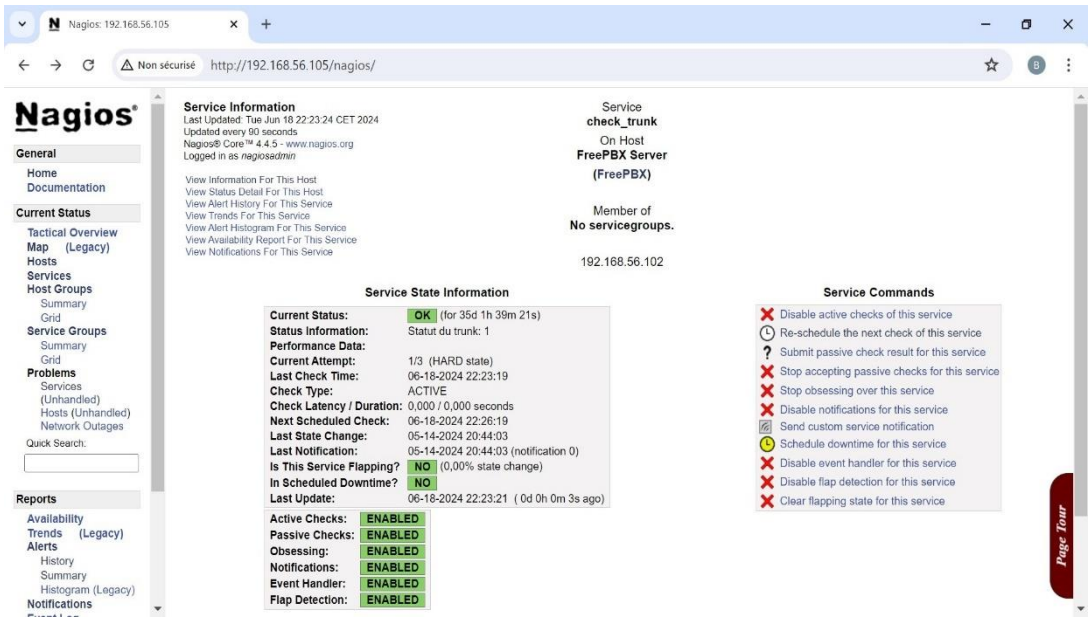


Figure IV. 32. check_trunk sur l'interface Nagios du FreePBX

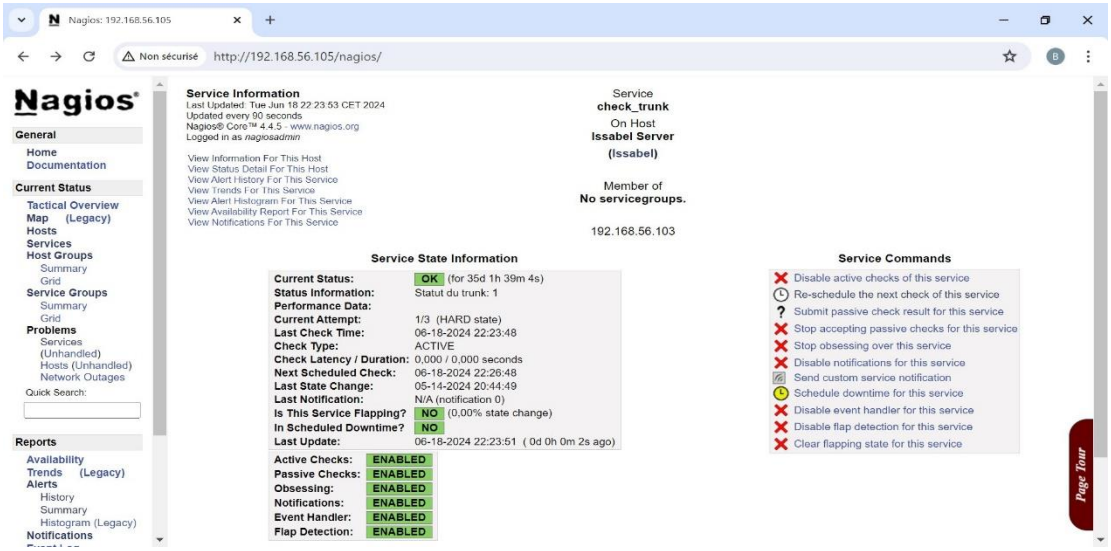


Figure IV.33. check_trunk sur l'interface Nagios du Issabel

IV.4.3.2. Supervision de Up phone et Down phone

Dans cette étape, nous surveillons le nombre de téléphones en ligne et hors ligne. Sachant que nous avons deux téléphones sur le serveur Issabel et deux autre sur FreePBX.

Sur les applications MicroSip et Zoiper, nous avons configuré et utilisé les extensions de l'un des serveurs, par exemple, FreePBX (4000 et 4001). Actuellement, nous supervisons le système pour vérifier que Nagios affiche correctement deux téléphones en ligne et aucun téléphone hors ligne.

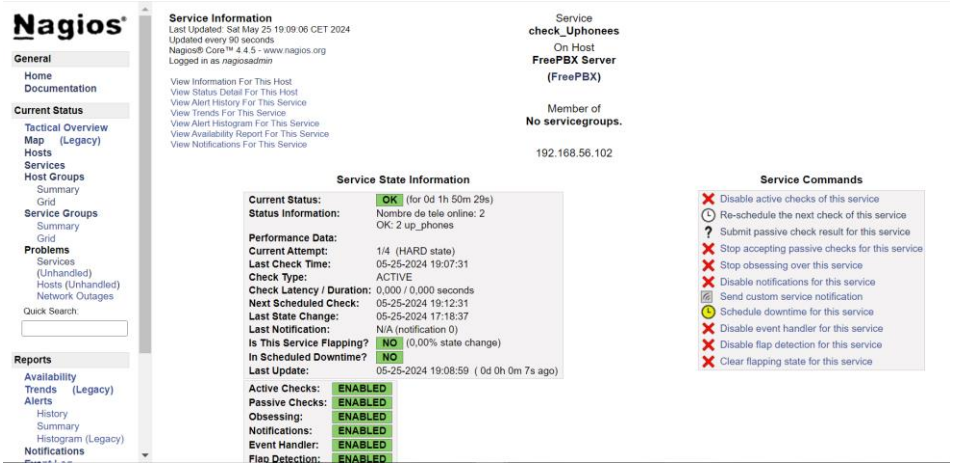


Figure IV.34. chek_Up phone sur l'interface Nagios du FreePBX.

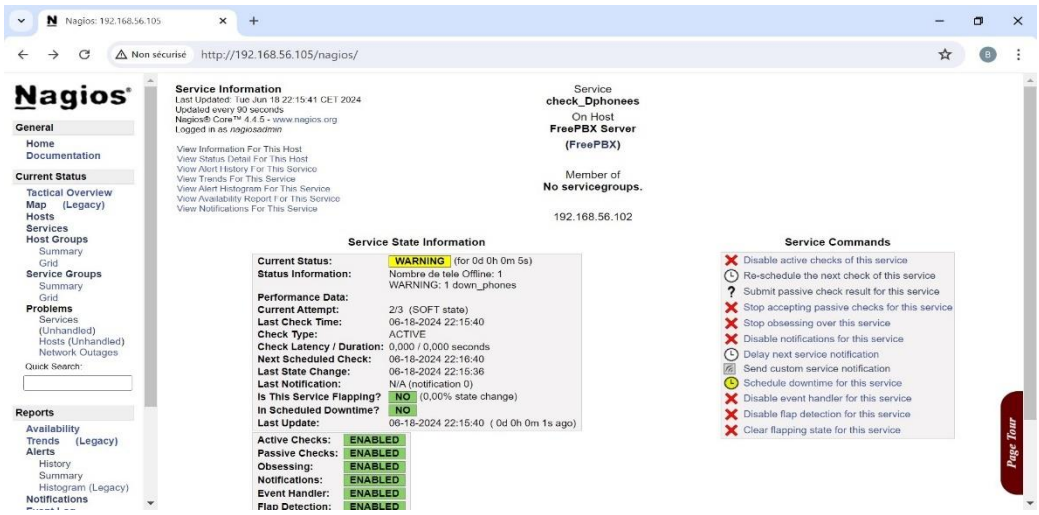


Figure IV.35. chek_Down phone sur l'interface Nagios du FreePBX

Les résultats de notre test initial confirment que le système fonctionne correctement.

Ensuite, nous allons déconnecter l'un des deux téléphones et vérifier si Nagios détecte et rapporte précisément ce changement de statut.

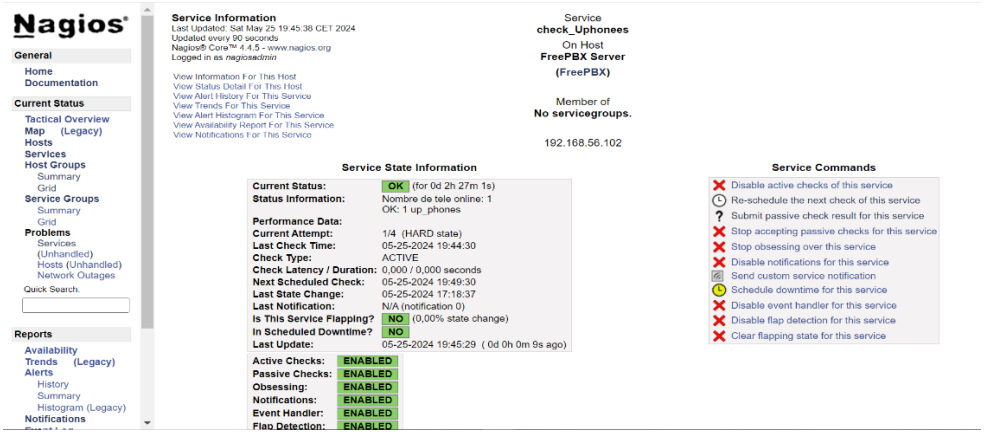


Figure IV.36. chek_Up phone sur l'interface Nagios du FreePBX

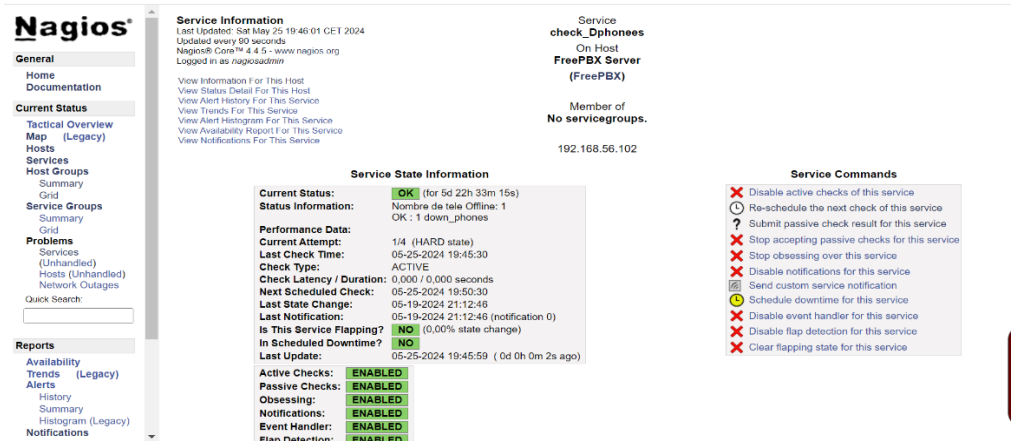


Figure IV.37. chek_Down phone sur l'interface Nagios du FreePBX

IV.4.3.3. Supervision d'Active calls

Cela signifie que notre serveur de supervision doit afficher les informations correctes concernant les appels en cours. Nous vérifierons que Nagios détecte et rapporte la présence d'un appel actif. Pour cela on va faire une appelle entre les deux serveurs et on test.

Figure IV. 38. Appelle entre serveur

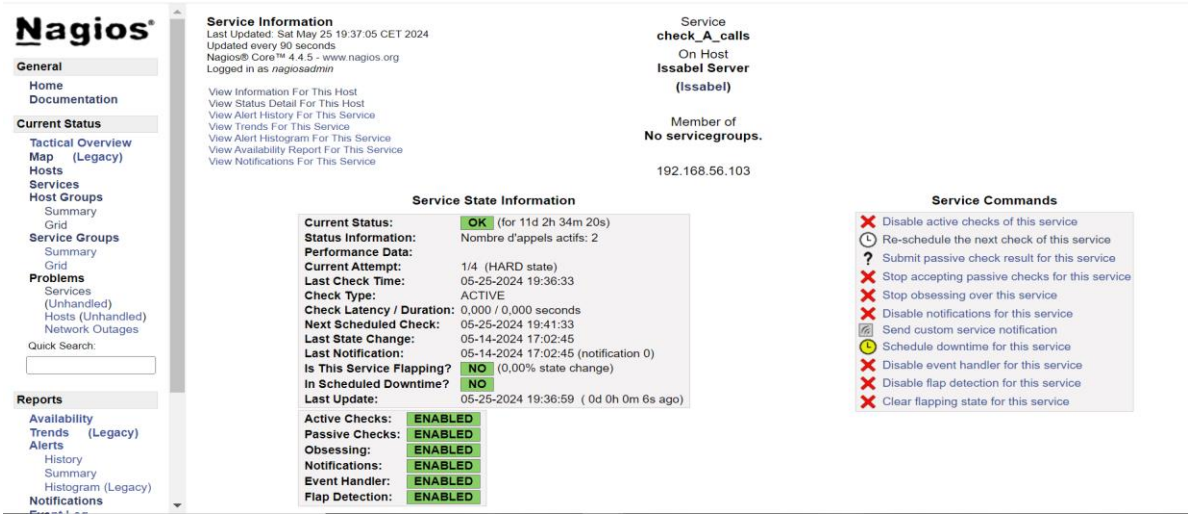


Figure IV. 39. Teste d'active calls

IV.4.4. Test des alertes

Dans cette étape, nous allons tester les alertes mail pour vérifier si elles fonctionnent lorsque notre réseau est en panne, c'est-à-dire en état critique.

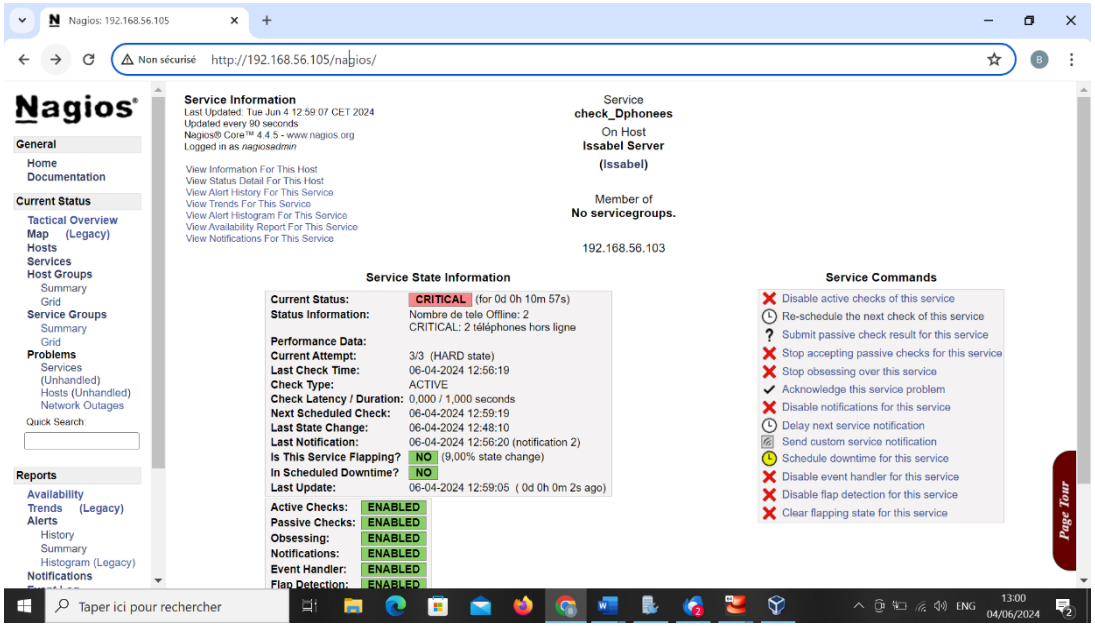


Figure IV.40. Etat Critical

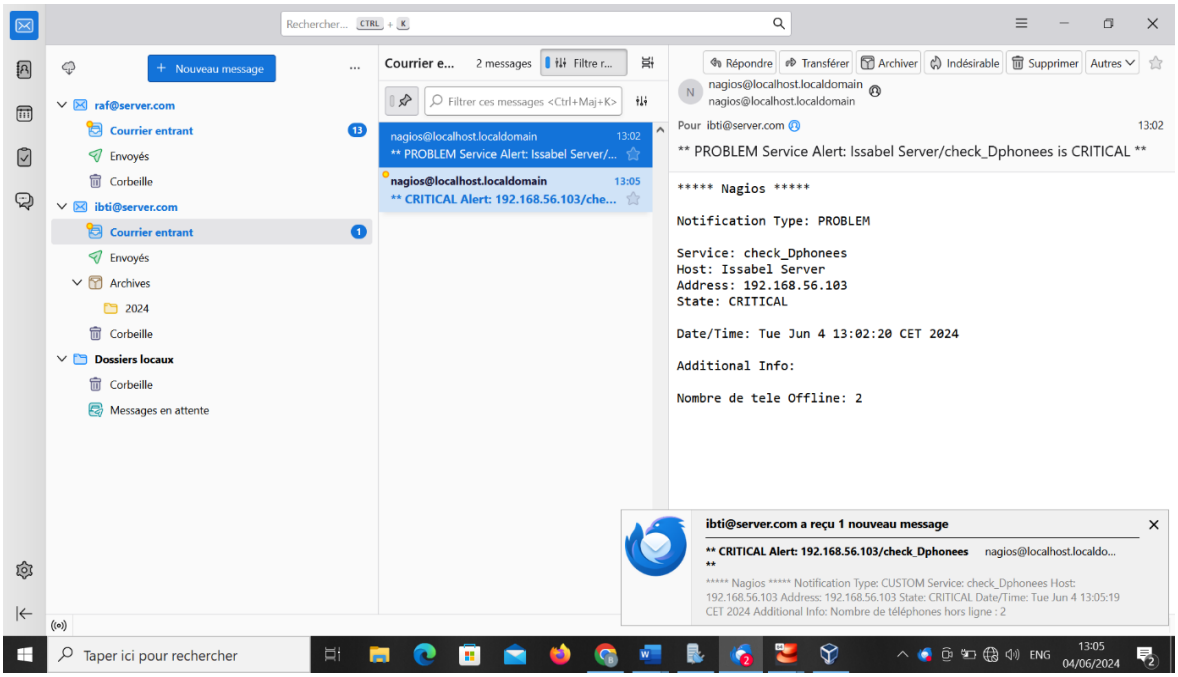


Figure IV. 41. Teste d'alerte

IV.5. Conclusion

Ce chapitre nous aide à comprendre comment intégrer divers composants logiciels pour créer un environnement de surveillance puissant, en mettant l'accent sur la configuration et l'interopérabilité des différents systèmes. Cela constitue la base d'une surveillance proactive et d'une gestion efficace de l'infrastructure VoIP, garantissant une disponibilité et des performances élevées. À l'avenir, nous pourrons améliorer notre projet en ajoutant une autre solution pour détecter les pannes, à savoir l'envoi de notifications par SMS aux personnes autorisées de notre entreprise.

CONCLUSION GÉNÉRALE

Au cours de ce projet, nous avons mis en place un système de supervision des infrastructures VoIP de SONELGAZ pour améliorer les communications internes et assurer la continuité des services. Pour y parvenir nous avons travaillé sur des logiciels open sources pour aboutir à une plateforme VOIP à base de FreePBX, Issabel riche en services de téléphonie sur IP et facilement extensible.

En premier lieu, nous avons procédé à une recherche théorique ciblée et concise pour comprendre les notions de base que traite ce projet, à savoir les avantages et les inconvénients de la technologie VOIP, ses architectures et ses protocoles.

En deuxième lieu, nous avons configuré un serveur de supervision, développé des scripts spécifiques pour chaque serveur téléphonique et conçu une interface utilisateur intuitive.

Les tests ont validé l'efficacité de cette solution, permettant une détection rapide des anomalies et une réactivité accrue grâce à un système d'alerte performant. Les notifications automatiques offrent une vue continue sur la performance des infrastructures, aidant à identifier rapidement les problèmes récurrents.

Ainsi, ce projet garantit la disponibilité et la fiabilité des infrastructures VoIP de SONELGAZ, tout en assurant une réactivité optimale face aux incidents, contribuant ainsi à la performance globale de l'entreprise et à la satisfaction de ses utilisateurs.

BIBLIOGRAPHIE

BIBLIOGRAPHIE

[1] : https://www.sonelgaz.dz/fr/category/qui-sommes-nous Consulter le 05/02/2024.

[2] : Formation d'intégration des nouvelles recrues (Société Algérienne de l'électricité et du gaz)

[3] : CHIKHAR DALEL, BESKRA Amet ellah moufida, Etude conception et réalisation d'un système d'information de la relève clientèle BT/BP, Master en informatique, Université Saad Dahleb Blida1.

[4] : Sébastien DÉON, VoIP et ToIP -Asterisk la téléphonie IP d'entreprise, 2007.

[5] : Mounir Kaali, La téléphonie sur IP avec 'ASTERISK', Rapport de stage, Université Mohammed V-Agdal, Ecole supérieure de technologie-Salé, 2012/2013.

[6] : M. ADNANE Nasser, M. MERSEL Nabyl, Etude et Mise en Place D'une Solution VoIP Sécurisée, Master en Informatique, Université Abderrahmane Mira de Bejaïa, 2016/2017.

[7] : https://sip.goffinet.org/sip/architecture/, Consulter le 02/03/2024

[8] :https://eduscol.education.fr/sti/sites/eduscol.education.fr.sti/files/ressources/pedagogiques/7420/7420-serveur-asterisk-protocole-ssh.pdf , Consulter le 05/03/2024

[9] :https://www.cisco.com/c/fr_ca/support/docs/voice/media-gateway-control-protocol-mgcp/214635-configure-and-troubleshoot-mgcp-gateways.html#to , Consulter le 10/03/2024

[10] : https://wikimemoires.net/2011/03/protocole-de-transport-de-voip-codecs/ , Consulter le 15/03/2024.

[11] :https://learn.microsoft.com/fr-fr/exchange/audio-codecs-exchange-2013-help#codecs, Consulter le 17/03/2024.

[12] : M. GADOUM Karim, M. AZOUAOUI Sofiane, Mise en place d'une solution VoIP à base de serveur Asterisk, Master en Electronique, Université MOULOUD MAMMERI TIZI-OUZOU, 2011/2012.

[13] : file:///C:/Users/BST/Downloads/t%C3%A9l%C3%A9chargement%20(1).htm , Consulter le 25/03/2024.

[14]:http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2001ttv02/Bidault-Hamon/CI4.htm, Consulter le 26/03/2024

[15] : https://upload.wikimedia.org/wikipedia/commons/e/e2/SIP-B2BUA-call-flow.png , Consulter le 02/04/2024.

[16]: file:///C:/Users/BST/Downloads/t%C3%A9l%C3%A9chargement%20(2).htm , Consulter le 02/04/2024.

[17]:https://www.lemondeinformatique.fr/publi_info/lire-voip-definition-fonctionnement-et-avantages-pour-une-entreprise-706.html, Consulter le 06/04/2024.

[18] : Nouri Lobna, Méchichi Amira, Implémentation du serveur de téléphonie (ASTERISK) Dans le cadre de projet de création d'un centre service client, Rapport de Projet de fin d'études, UNIVERSI VIRTUELLE DE TUNIS, 2010/2011.

[19] : https://www.sangoma.com/asterisk-freepbx-difference/ , Consulter le 09/04/2024.

[20] : https://docs.asterisk.org/Configuration/Applications/Voicemail/,Consulter le 09/04/2024.

[21] : https://docs.asterisk.org/

[22] : https://www.asterisk.org/get-started/applications/gateway/, Consulter le 11/04/2024.

[23] : https://www.slideshare.net/bamaemmanuel/etudes-et-dploiement-dune-solution-voip-base-sur-asterisk , Consulter le 12/04/2024.

[24] : https://mhoungbo.fedorapeople.org/ambassador/Projet%20devoir%20VOIP.pdf, Consulter le 05/05/2024.

[25] : http://archives.univ-biskra.dz/bitstream/123456789/11061/3/MEZHOUDI-YAZID.pdf, Consulter le 15/04/2024.

[26] :https://www.univbejaia.dz/dspace/bitstream/handle/123456789/8762/Interconnexion%20de%20deux%20serveurs%20Asterisk%20et%20mise%20en%20place%20de%20t%C3%A9l%C3%A9phonie%20et%20visiophonie%20sur%20IPCas%20d%E2%80%99%C3%A9tude%20%20Facult%C3%A9%20des%20sciences%20exactes%20et%20ses%20d%C3%A9partements?isAllowed=y&sequence=1, Consulter le 22/04/2024.

[27] : HADJ ALI Mehdi, DJENAOUCINE Anis, Realisation d'une solution VoIP avec le serveur FreePBX, Rapport de Projet de fin d'études, Master en Informatique,Universite A/Mira de Bejaia, 2021/2022.

[28]: Alex Robar, FreePBX 2.5 Powerful Telephony Solutions, Packt Publishing,2009

[29]: https://www.issabel.org/, Consulter le 28/04/2024.

[30]: https://fr.slideshare.net/slideshow/formation-elastix/84986661, Consulter le 06/05/2024.

[31]:https://fcmicro.net/supervision-informatique-tout-ce-quil-faut-savoir/, Consulter le 08/05/2024

[32]: https://www.keyyo.com/fr/telephonie-ip/supervision, Consulter le 10/05/2024.

[33]:https://www.axialys.com/fonctionnalites-centrex/supervision-telephone/, Consulter le 12/05/2024.

[34]: https://fr.slideshare.net/christedykeihouad/projet-technique-licence-christedy, Consulter le 15/05/2024.

[35]: https://www.google.com/url?sa=i&url=http%3A%2F%2Fportfolio-valentinrobion.weebly.com%2Fuploads%2F5%2F2%2F1%2F8%2F52187501%2Fdoc_monitoring.pdf&psig=AOvVaw0VqNYoK7yctWziDcGoYnQC&ust=1715887145261000&source=images&cd=vfe&opi=89978449&ved=0CBAQjRxqFwoTCOimpPKvkIYDFQAAAAAdAAAAABAR, Consulter le 18/05/2024.

[36] : https://www.ringover.fr/blog/toip , Consulter le 14/06/2024.