REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'enseignement Supérieur et de la Recherche Scientifique

Université M'HAMED BOUGARA– BOUMERDES

Faculté des sciences
Département de physique

Domaine : Sciences et Techniques
Filière : Génie Electrique
Spécialité : Réseaux et télécommunications

MEMOIRE DE FIN D'ETUDE
Pour l'obtention du diplôme de
MASTER

Thème :

Monitoring du réseau d'Algérie Poste via l'outil Cisco Prime Infrastructure

Par :

- BOUZAD Rym
- OUMOHAND Massylia

Encadré par :

- Mr Med Amine RIAHLA

Jury:
- **Mr Yassine MERAIHI**
- **Mme Samira MECHID**
- **Mr Med HAMADOUCHE**

Année universitaire : 2017/2018

Avant de commencer la présentation, on profite de l'occasion pour remercier du profond de notre âme ALLAH qui nous a permis d'arriver au terme de ce travail.

Toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce projet de fin d'études.

Nous tenons à exprimer notre gratitude à notre encadreur ***Dr RIAHLA Med Amine.*** *On le remercie de nous avoir encadré, orienté, aidé et conseillé.*

Nous tenons à remercier, les membres du jury de nous avoir honoré en acceptant de juger notre travail.

Une mention spéciale à ***Mme Radia BOUHOUNE, Mlle Sabrina OULDMOHAMMED,*** *et* ***Mr Salem GUESMI*** *pour leur accueil, leur aide et leur bienveillance durant notre période de stage.*

Nos remerciements les plus profonds à tous nos professeurs, enseignants et toutes les personnes qui nous ont soutenus jusqu'au bout.

Rym & Massylia

Je dédie ce modeste travail

*A mes très **chers parents** et ma **grand-mère**, qui ont toujours été là pour moi, « Vous avez tout sacrifié pour vos enfants n'épargnant ni santé ni efforts. Vous m'avez donné un magnifique modèle de labeur et de persévérance. Je suis redevable d'une éducation dont je suis fière ».*

*A mon cher et **unique frère Latamene**, et mes chères **sœurs Zahia, Sabah, Dahbia, Souhila, Sarah, Katia** et enfin notre petite **Lydia,** qui m'ont soutenu sans cesse.*

*A mes **beaux-frères Farid, Mouloud, Arezki** et ma **belle-sœur Tassadit** que j'estime beaucoup.*

*A mes **neveux** et **nièces** que j'aime tant **; Massin, Cilia, Ania, Yanis, Selyan, Melissa, Dalia, Sarah, Nelia, Ilyes, Amélia Baya** & **la petite** qui va nous rejoindre bientôt.*

*A **Amir** qui m'a encouragé et soutenu durant mon cursus.*

*A mon **binôme, meilleure amie Rym** pour ses efforts fournis, son courage et sa présence permanente*

*A mes merveilleuses meilleures amies **Ryma & Sihem.***

***A** mes chères amies **Rania & Nesrine**.*

*Enfin, à mes **Ami(e)s** et **camarades** de promotion.*

A vous tous, je vous présente mes remerciements, mon respect et ma gratitude.

Massylia

Dédicace

Avec tout respect et amour que je dédie ce mémoire

A mes très chers parents

Pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études ;

Je prie le bon Dieu de les bénir, de veiller sur eux, espérant qu'ils seront toujours fièrs de moi ;

A mes chères sœurs Ibtissem, Warda et Asma pour leurs encouragements permanents, et leur soutien moral ;

A mes deux petits frères ABD Raouf et Med Mouloud pour leur appui,

A mes beaux-frères Nabil et Zakaria ;

A mon adorable neveu Aymen et ma petite nièce Cyrine ;

Une mention très spéciale à ma chère tante Hnifa et son mari ;

A mon binôme, meilleure amie, sœur Massylia, pour son soutien, son encouragement, et surtout pour sa présence chaleureuse et bienveillante ;

A mes plus belles rencontres de ces cinq dernières années Rania et Nesrine,
Pour leurs soutiens et encouragements ;

A ma meilleure amie Fayrouz,
En souvenir des plus beaux instants qu'on a passés ensemble ;

A toute ma famille pour leur soutien tout au long de mon parcours universitaire ;

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible ;

Merci d'être toujours là pour moi.

Rym

Sommaire

Chapitre II : Généralités sur les réseaux d'entreprise

Chapitre III : Monitoring avec l'outil de Cisco Prime Infrastructure

Chapitre IV : Mise en place de l'outil Cisco Prime infrastructure 2.2

Liste des figures :

Liste des tableaux :

Introduction générale :

Actuellement, les systèmes d'informations dans les entreprises deviennent de plus en plus importants mais aussi complexes.

Le besoin de maintenance et de gestion de ces systèmes est rapidement devenu une priorité. Plusieurs logiciels de surveillance et de supervision de réseaux ont été développés pour vérifier l'état du réseau en temps réel et pour être informé au plutôt de tout incident réseau. Grâce à ces logiciels, les délais d'interventions sont fortement réduites et les anomalies peuvent être aussitôt prises en main sans que les utilisateurs du réseau en question soient affectés ou remarquent des erreurs.

La supervision va consister à établir des points de contrôle sur différents éléments du parc IT, qu'ils soient matériels, applicatifs, ou bien des interconnections. Cette technique d'observation va permettre d'utiliser au mieux les ressources informatiques et obtenir l'état des réseaux ainsi que leur comportement en temps réel ou de manière pro active.

Problématique :

A ce jour la visualisation du réseau d'Algérie Poste était faite avec Nagios. Présentant beaucoup de fonctionnalités mais aussi des inconvénients qui ont poussé le personnel de ce domaine à opter pour un outil meilleur en termes de performance.

Ces inconvénients sont :

- Difficulté à installer et à configurer ;
- Interface compliquée ;
- Ne permet pas d'ajouter des hosts via Web ;
- Besoin d'un autre outil comme CACTI pour faciliter sa configuration ;
- Pas de representations graphiques ;

- Les mises à jour de la configuration se font en mode « lignes de commandes » et doivent être réalisées côté supervision comme côté serveur à superviser.

Cette étude consiste à installer et configurer l'outil de supervision Cisco Prime afin d'identifier le réseau entier et le visualiser. Cette visualisation comprend aussi la vérification de l'état des éléments d'interconnexion ainsi que la réception des alertes concernant leur disponibilité et leur validité.

Une étude de cet outil est nécessaire pour promouvoir sa bonne configuration et son bon fonctionnement pour un rendement meilleur dans la gestion du réseau de cette entreprise.

Méthodologie :

L'approche méthodologique de la problématique posée est structurée en quatre parties :

Chapitre I : Présentation de l'organisme d'accueil (Direction Générale d'Algérie Poste) et étude de l'existant, qui introduit les composants du réseau de l'entreprise en termes d'architecture, d'équipements et systèmes reliant les différentes sous directions et bureaux au niveau national.

Chapitre II : Généralités sur les réseaux d'entreprise : introduit les équipements, les services et protocoles de communications.

Chapitre III : Monitoring avec l'outil Cisco Prime Infrastructure : introduisant le concept du monitoring et le SNMP en général et plus exactement Cisco Prime Infrastructure.

Chapitre IV : Mise en place de l'outil Cisco Prime Infrastructure : Présente les différentes étapes d'installation, post-installation et de configuration de cet outil ainsi que les différentes configurations faites pour la réalisation de notre projet.

L'analyse par parties est ponctuée par une conclusion générale et des propositions de perspectives.

Par ailleurs, les outils pédagogiques utilisés dans cette démarche méthodologique ont trait aux acquis théoriques appliqués et par la consultation des ouvrages appropriés ainsi que les publications écrites ou diffusées par internet.

Introduction :

La visualisation de l'ensemble du réseau nécessite une très bonne connaissance de l'entreprise et son environnement informatique qui aide à déterminer la portée du projet d'implémentation de la solution.

Dans ce premier chapitre nous présenterons les principales missions, ressources, et la structure d'Algérie poste ainsi que l'architecture réseau de l'entreprise.

Partie I : Présentation de l'organisme d'accueil :

I.I.1 Présentation

Suite à la restructuration du secteur de la poste et des télécommunications selon la loi 2000-03 du 05 août 2000, il a été créé par décret exécutif n° 02-43 du 14 janvier 2002 un établissement public national à caractère industriel et commercial (EPIC) dénommé « Algérie Poste ».

C'est une entreprise Algérienne publique chargée d'assurer, sur l'ensemble du territoire national la mise en œuvre de la politique nationale de développement des services postaux et des services financiers postaux à travers la prise en charge des activités de gestion des présentations, de renouvellement et de développement des infrastructures s'y rapportant.

I.I.2 Missions

Algérie Poste assure les activités traditionnelles dévolues du courrier et colis, des services financiers (paiement des salaires, pension, épargne, allocations...) et assure des prestations diverses : location cases postales, vente d'annuaires, vente de timbres fiscaux, amendes vignettes, remboursement biens d'équipements. Pour le compte d'entreprises : paiement des factures (SONELGAZ, SEEAL, ATM MOBILIS, ORASCOM ALGERIE TELECOM).

En développement, logistique transport et e-logistique, opérations commerciales via le Net (e-commerce), un espace boutique dans les bureaux de poste et de la distribution de la presse (messagerie).

I.I.3 Ressources

Pour l'année 2012 Algérie poste a enregistré :

- ✓ 3398 bureaux de poste et 10752 guichets dans le territoire national.
- ✓ Une densité postale de 10471 habitants par bureau et 4679 habitants par guichet.

- ✓ 13,5 millions de comptes CCP et 333 millions d'opérations.
- ✓ 33,3 milliards de DA d'opérations de débit-crédit CCP.
- ✓ 3,9 millions de comptes CNEP et 2,5 millions d'opérations.
- ✓ 200 millions de postes aux lettres et 523 000 colis.
- ✓ 5 816 691 porteuses de cartes magnétiques.
- ✓ 1 centre national des chèques postaux.
- ✓ 6 centres régionaux des chèques postaux.
- ✓ 310 millions d'objets traités/an.
- ✓ 450 000 colis traités /an.
- ✓ Plus de 1 million de visiteurs par jour.

I.I.4 Structure

Algérie poste est constituée de deux principales divisions :

I.I.4.1 Division administrative d'Algérie poste

La structure organisationnelle d'administration d'Algérie poste est bâtie sur les niveaux suivants :

I.I.4.1.1 La direction générale :

La direction générale met en œuvre les orientations et délibérations du conseil d'administration, dans ce cadre, elle dispose des pouvoirs les plus étendus pour assurer la direction et la gestion administrative, technique et financière de l'établissement.

La direction générale est composée de :

I.I.4.1.1.1 Direction opérationnelle :

Elle est concernée par tout ce qui est postale, finance, comptabilité, moyens, ressources, commerce et informatique.

I.I.4.1.1.2 Direction d'étude :

C'est une direction qui fait des études sur de différents domaines : management de la qualité, stratégie, planification, organisation, contrôle de gestion et de l'audit interne, communication…etc.

I.I.4.1.2 Centre Financier Régional (CFR) :

Il se compose principalement de 08 centres régionaux :

CFR d'Alger, CFR d'Oran, CFR de Annaba, CFR de Chlef, CFR de Sétif, CFR de Ouargla, CFR de Béchar, et enfin CFR de Constantine.

Chaque CFR a compétence sur l'ensemble des UPW relevant de son territoire.

I.I.4.1.3 L'Unité Postale de Wilaya (UPW) :

Les unités postales de wilaya sont au nombre de 48 (une unité pour chaque wilaya). Chaque unité a compétence sur l'ensemble des bureaux de poste (BP) de la wilaya, ainsi elle est chargée :

- ✓ D'exécuter les programmes de développement et d'élaborer les rapports périodiques sur les activités de la wilaya.
- ✓ De gérer l'infrastructure et l'exploitation postale de la wilaya.
- ✓ D'informer la direction territoriale des postes sur toutes violations du régime de l'exclusivité.
- ✓ D'exécuter les programmes d'inspection.
- ✓ De procéder au recensement et à la validation du patrimoine mobilier et immobilier de la wilaya.
- ✓ De mener des actions de communication et réaliser des manifestations dans le but de promouvoir les produits d'Algérie poste au niveau de la wilaya.

Organigramme général d'Algérie poste :

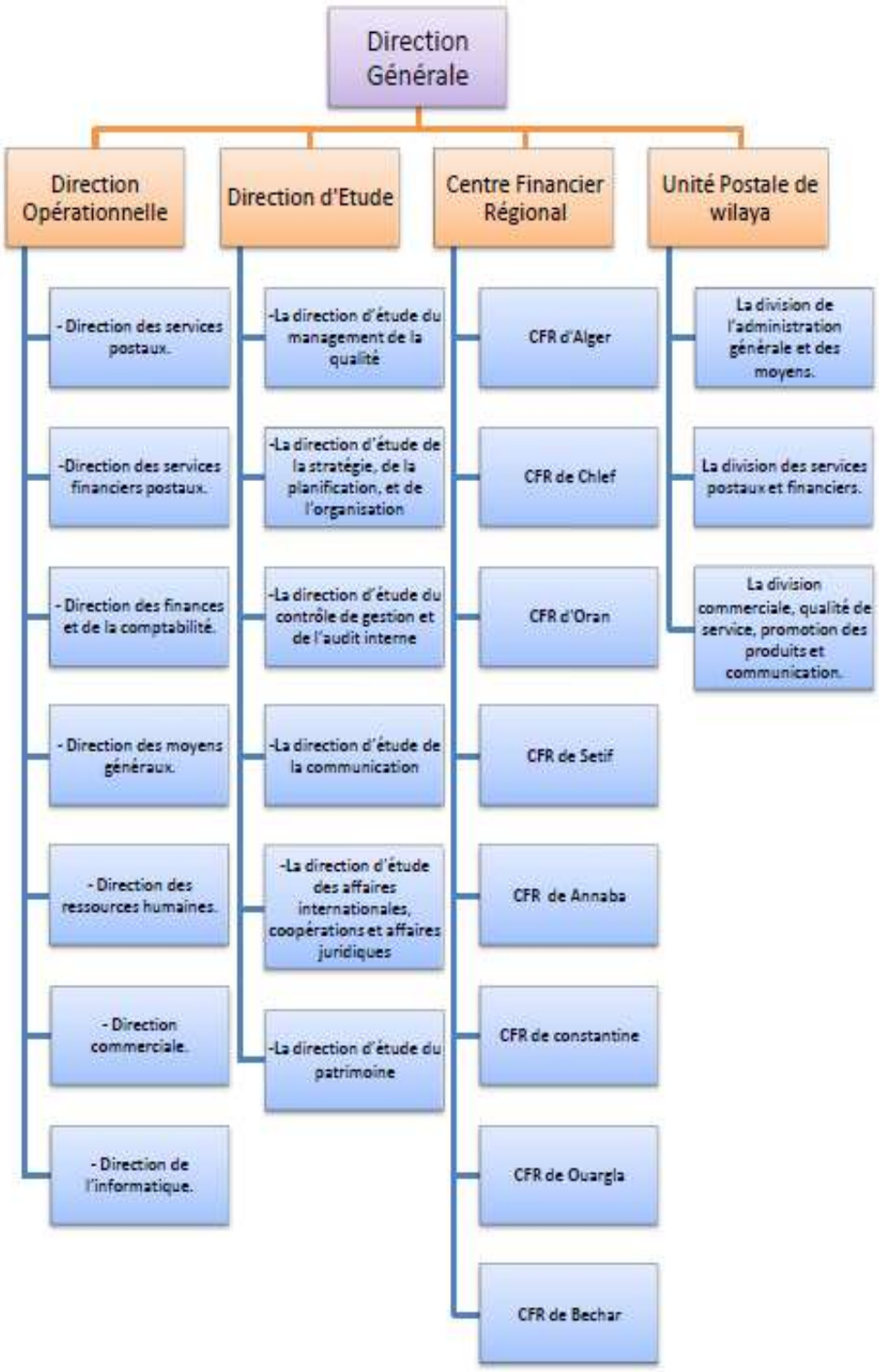


Figure 01 : Organigramme général d'Algérie Poste

I.I.4.2 Division fonctionnelle d'Algérie poste

Algérie poste s'est divisée selon ses différentes fonctions en quatre divisions :

I.I.4.2.1 Division monétique :

Elle assure tout ce qui concerne la monétique, toutes les fonctions traditionnelles et même moderne, elle se divise à son tour selon le type d'opérations :

I.I.4.2.1.1 Les comptes courants postaux (CCP) :

Ce sont les comptes ouverts pour une entreprise ou un particulier sur lequel ont lieux des opérations de dépôt ou de retrait d'argent.

I.I.4.2.1.2 Les comptes de la caisse nationale d'épargne et de prévoyance (CNEP) :

Algérie poste est prestataire de services pour le compte de la Caisse Nationale d'épargne et de Prévoyance (CNEP) par la mise à disposition de son parc de bureaux de poste, c'est un service qui offre au client une possibilité de verser un tant d'argent à son compte CNEP avec un pourcentage d'intérêt à long ou à court terme.

I.I.4.2.1.3 Les mandats :

C'est un type de la division monétique qui permet d'envoyer à un tiers une somme illimitée d'argent, il existe plusieurs types de mandats où on peut citer :

-mandat carte, transfert de fonds entre particuliers,

-mandat d'impulsion à un CCP,

- mandat payable à un particulier par débit d'un CCP,

-mandat télégraphique.

I.I.4.2.2 Division Réseau :

Elle concerne toutes les activités des bureaux de poste, et elle permet de déterminer la classe des bureaux de poste selon l'activité, l'effectif et le chiffre d'affaire. En effet il existe huit classes des bureaux de poste : RP, R1, R2, R3, RCE, RHE, RHS, RHC qui sont triées par ordre décroissant.

I.I.4.2.3 Division Informatique :

C'est une division qui sert à transmettre les informations entre les différentes divisions, à fournir les moyens et à assurer le contacte entre les différents bureaux de poste, ainsi qu'à fournir le matériel électronique.

I.I.4.2.4 Division courrier colis :

Elle assure le transport des courriers et des colis, ainsi que la fabrication et la vente des timbres.

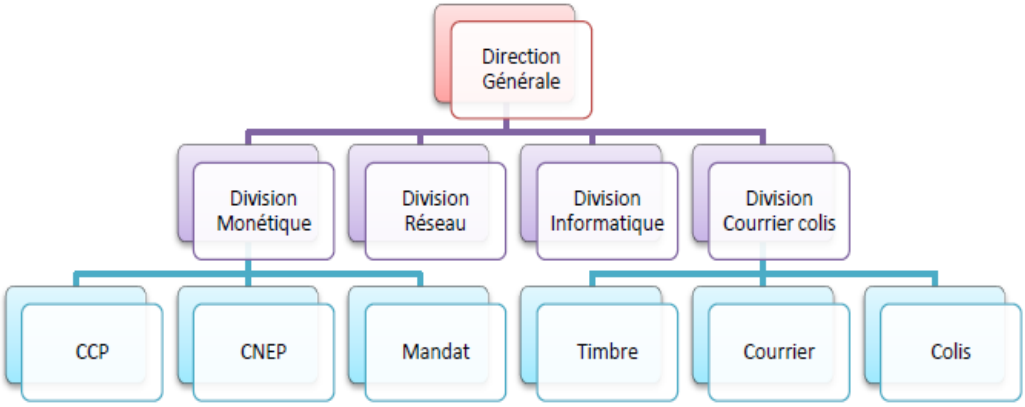


Figure 02 : Organigramme général des fonctions

I.I.5 L'élaboration des statistiques à Algérie poste

Chaque fin de mois, Algérie poste élabore des statistiques concernant toutes les transactions effectuées pendant le mois dans tous les bureaux de poste de l'Algérie.

Le flux de transportation des informations se décrit comme suit :

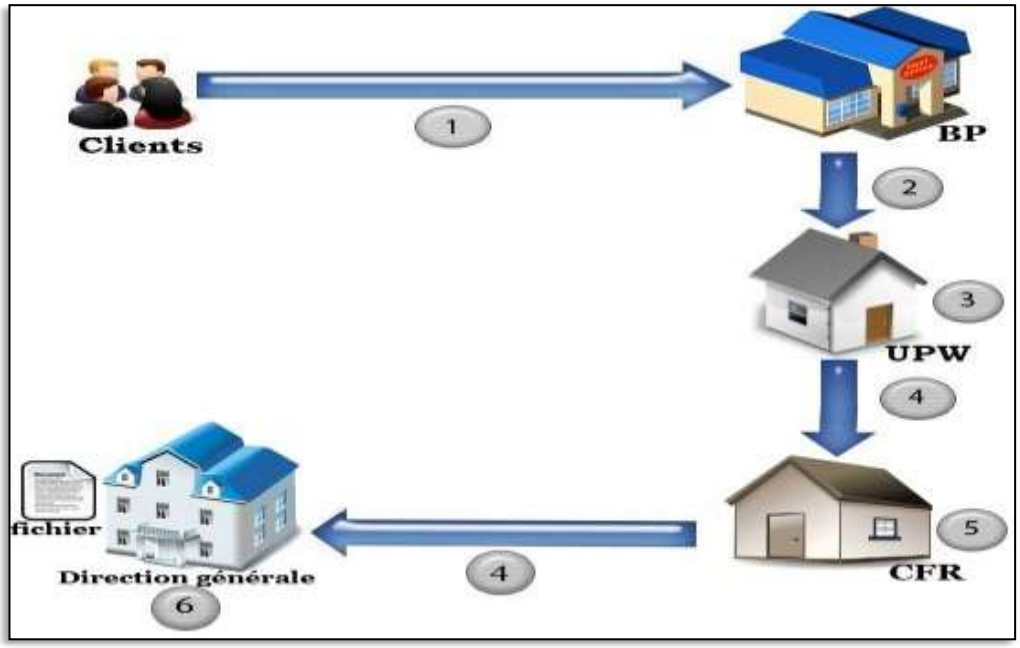


Figure 03 : Déroulement des transactions et l'élaboration des statistiques à Algérie poste

- Faire les différentes opérations des bureaux de poste.
- Envoyer taxe, nombre et montant de toutes les opérations effectuées pendant le mois.
- Collecter toutes les informations qui parviennent des BP dans un seul fichier.
- Envoyer le fichier.
- Collecter toutes les informations qui parviennent des UPW dans un seul fichier
- Collecter et archiver toutes les informations qui parviennent des CFR dans un seul fichier afin de l'utiliser dans l'élaboration des différentes statistiques.

Partie II : État de l'existant :

II.1 Présentation :

Dans cette partie, nous déterminerons l'architecture globale de la direction d'Algérie poste ainsi que l'infrastructure système (serveurs, routeurs, BP, POP, LS et centre de données).

La figure 01 illustre cette architecture qui ne présente que les bureaux de postes(BP) principaux (BP Oran, BP Ouargla, BP Bechar, BP Adrar, BP Sétif, BP Annaba, BP Birtouta et la Direction générale) afin de faciliter la compréhension de cette dernière.

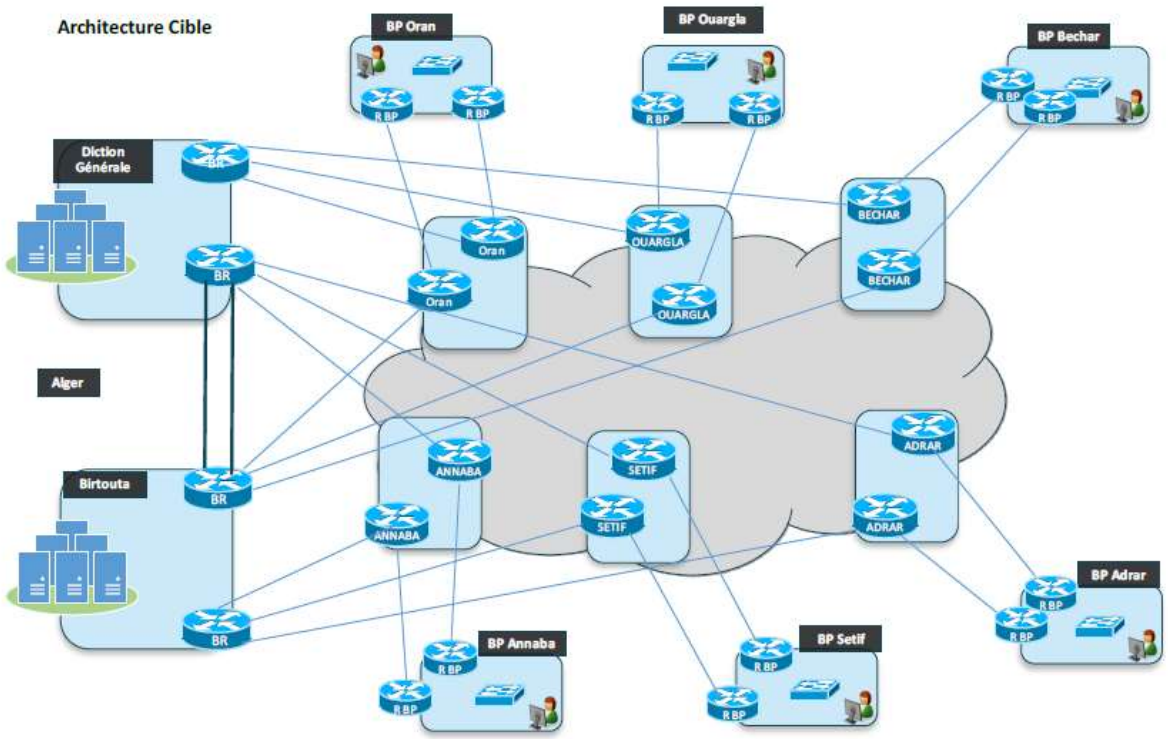


Figure 04 : Architecture globale d'Algérie poste

II.2 Explication de l'architecture :

- Le réseau d'Algérie poste se décompose en 4 régions (CENTRE, EST, OUEST et SUD) chaque région regroupe des wilayas qu'on appelle des UPW (Unité Postale Wilaya).
- Dans chaque région se trouve deux routeurs (ASR 1004) qu'on appelle PoPs régionaux (point of presence) et qui sont reliés via des VLANs
- Dans chaque UPW se trouve deux PoPs qui sont eux aussi relies via des VLANs.
- La liaison entre les UPW et les bureaux de poste est assurée par une liaison physique qu'on appelle LS (liaison spécialisée) configurée par Algérie Télécom sur un routeur « ASR 1001 »
- On trouve dans chaque bureau de poste un seul routeur (ASR 4221), switch et des utilisateurs.

La Direction générale d'Algérie Poste, utilise NAGIOS comme outil de supervision, cependant les administrateurs ont choisi de le changer à cause des points faibles de ce dernier qui sont :

- Difficulté à installer et à configurer ;
- Interface compliquée ;
- Ne permet pas d'ajouter des hosts via Web ;
- Besoin d'un autre outil comme CACTI pour faciliter sa configuration ;
- Pas de representations graphiques ;
- Les mises à jour de la configuration se font en mode « lignes de commandes » et doivent être réalisées côté supervision comme côté serveur à superviser.

Les administrateurs ont opté pour l'outil Cisco Prime Infrastructure 2.2 afin de superviser le réseau de l'entreprise. Leur choix s'est basé sur le concept du « Bring Your Own Device » qui permet aux collaborateurs de pouvoir travailler comme ils le souhaitent, quand et où ils le veulent, en ayant recours à n'importe quel équipement mobile.

Les points forts de ce dernier préconisent une approche complète présentant un triple intérêt comme suit :

- Une politique unifiée sur tous les réseaux LAN filaires ou sans fil, cellulaires et VPN, grâce aux améliorations apportées à la solution Cisco Identity Services Engine (ISE). Cette innovation permet à la fois de simplifier le « auto-enregistrement » des appareils utilisateurs et d'intégrer les politiques à des solutions de gestion des appareils mobiles (MDM).

- Une expérience utilisateur optimale sur l'ensemble du réseau filaire/sans fil. Les mises à jour de l'infrastructure permettent de doubler les capacités d'adaptabilité vidéo pour la multidiffusion, de prendre en charge jusqu'à 30 000 appareils à l'aide d'un seul contrôleur et de fournir une assistance IPv6 pour les appareils clients. De plus, elles contribuent à accroître les capacités vidéo haute qualité des solutions Cisco WebEx et Cisco Jabber.
- Une gestion simplifiée et centralisée des opérations, afin de mieux répondre aux attentes des utilisateurs en matière de performances applicatives, d'accélérer la résolution des pannes et de réduire les coûts opérationnels.

Conclusion partielle :

Ce premier chapitre nous a permis de connaitre l'organisme d'accueil, de comprendre l'environnement informatique de l'entreprise, dans le but de mieux gérer notre problématique en remplaçant un ancien outil de supervision ayant des points faibles considérables, par un autre plus performant, présentant des avantages bénéfiques pour l'entreprise.

Introduction :

Les réseaux informatiques sont de plus en plus vastes et complexes. Par ailleurs, leur administration est plus rude et demande beaucoup d'efforts.

En effet, toute interruption ou disfonctionnement dans les réseaux peut avoir des conséquences colossales.

Les administrateurs réseaux exécutent un ensemble de tâches de gestion et configuration afin de pouvoir assurer le bon fonctionnement de ces réseaux.

Dans ce qui suit, nous présenterons de façon générale les équipements sur lesquels un administrateur réseau effectue ses tâches afin d'assurer le bon fonctionnement des éléments d'interconnexion ainsi qu'une bonne communication.

II.1 Qu'est-ce qu'un réseau informatique ?

Un réseau est un ensemble d'équipements électroniques interconnectés, capable de communiquer par l'intermédiaire d'un support de communication. Il permet l'échange des informations et l'accès aux ressources de certains ordinateurs du réseau. [1]

II.2 Classification des réseaux :

On peut classifier les réseaux selon deux aspects :

- Leurs tailles.
- Leurs topologies.
    - ✓ Selon leurs tailles :

En fonction de la localisation, la distance et le débit, les réseaux sont classés en trois types :

• LAN (Local Area Network) : permet l'échange de données et le partage de ressources dans une entreprise

La distance de câblage est de quelques centaines de mètres.

• MAN (Métropolitain Area Network) : permet l'interconnexion des entreprises ou des départements sur un réseau spécialisé à haut débit.

• WAN (Wide Area Network) : réseau à l'échelle d'un pays, généralement celui des opérateurs. Le plus connu des WAN est Internet.

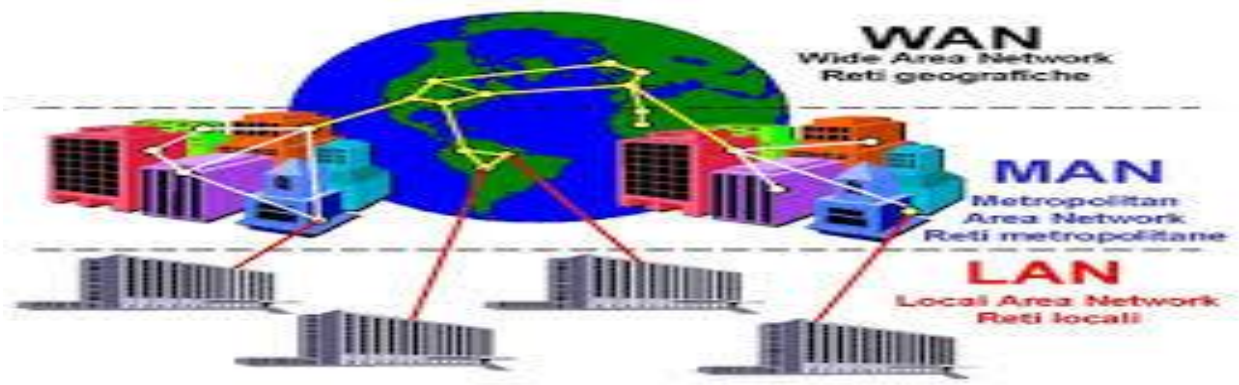


Figure 05 : les différents types d'un réseau informatique [4]

- ✓ Selon leur topologie :

La topologie est l'organisation physique et logique d'un réseau.

- L'organisation physique : concerne la façon dont les machines sont connectées (Bus, Anneau, Étoile, Maillé, ...)
- L'organisation logique **:** montre comment les informations circulent sur le réseau (diffusion, point à point) [2]

II.3 Les équipements d'interconnexion des réseaux :

- Pour l'établissement d'un réseau local il est indispensable d'interconnecter les ordinateurs d'une organisation.
- Dans le cas de réseaux homogènes il y'a aucun problème, par contre, dans le cas contraire c'est à dire quand les protocoles sont différents il faut procéder à une conversion de ces derniers. [1]

On distingue plusieurs équipements d'interconnexion :

II.3.1 Répéteur: permettent de régénérer un signal lorsque la distance qui sépare deux périphériques est longue, utilisé pour étendre la distance de câblage d'un réseau.

Figure 06 : Répéteur [5]

II.3.2 Le commutateur (Switch) : est un pont multi ports, il relie plusieurs segments physiques (câble ou fibre), c'est un équipement configuré de manière à gérer une ou plusieurs stations par port et peut gérer simultanément plusieurs liaisons.

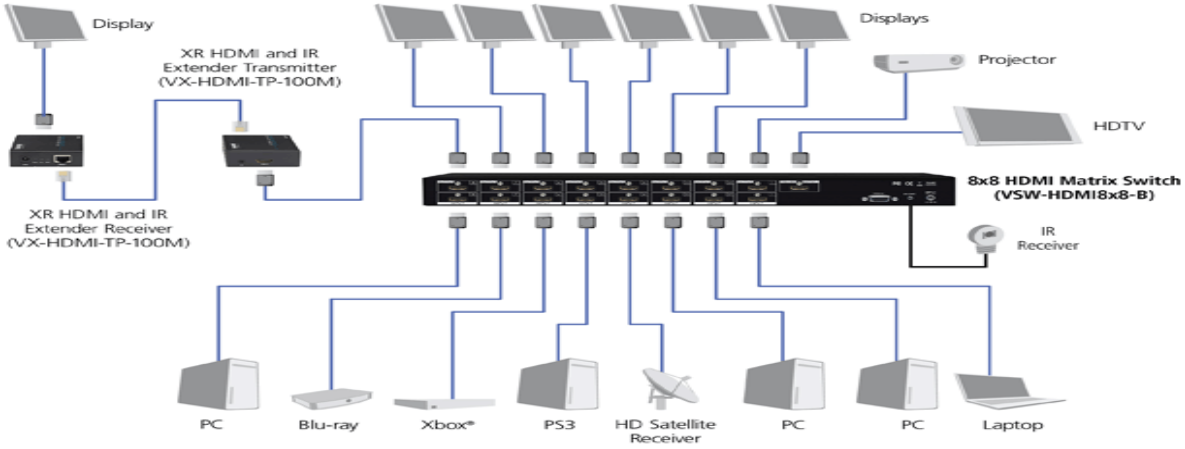


Figure 07 : Switch [5]

II.3.3 Le routeur : permet de choisir le meilleur chemin qu'un message va emprunter. Il est généralement utilisé pour l'interconnexion des réseaux à longue distance. Il est surtout employé pour l'interconnexion de plusieurs réseaux de types différents.

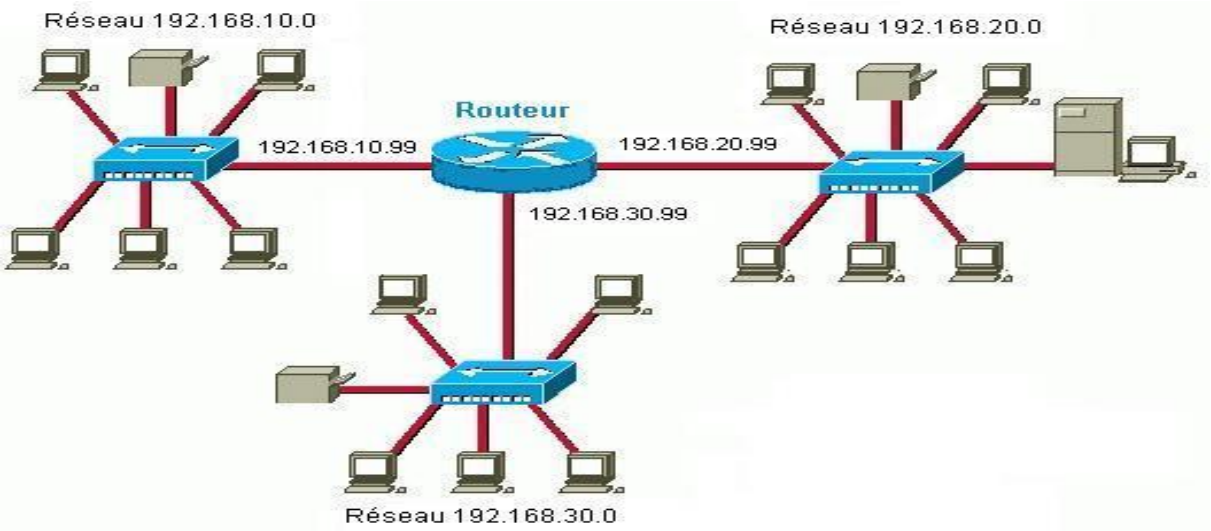


Figure 08 : Routeur [5]

II.3.4 pare-feu firewall : est un logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il mesure la prévention des applications et des paquets. [5]

II.3.5 La passerelle : permet d'interconnecter deux réseaux totalement différents, en assurant toutes les conversions de protocoles pour garantir les échanges entre deux réseaux.

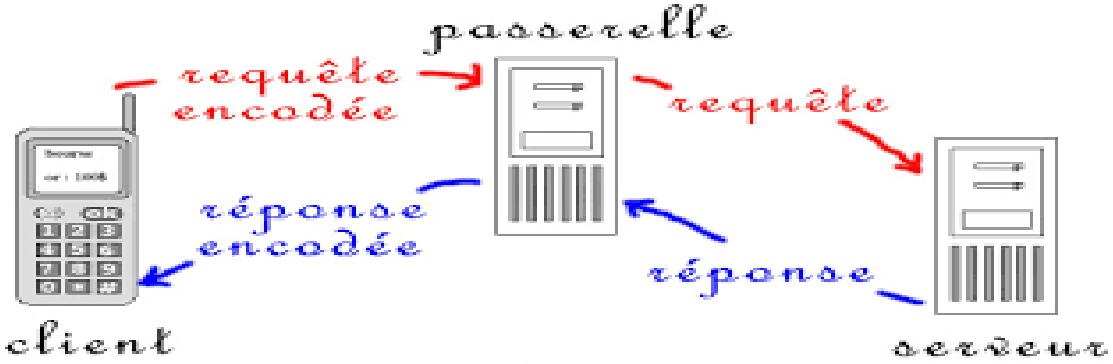


Figure 09 : Passerelle [5]

II.3.6 le Modem (modulateur-démodulateur) : sert à communiquer avec des utilisateurs distants. Il permet l'échange (envoi/réception) des fichiers, des fax, de se connecter à Internet, de recevoir et d'émettre des e-mails.

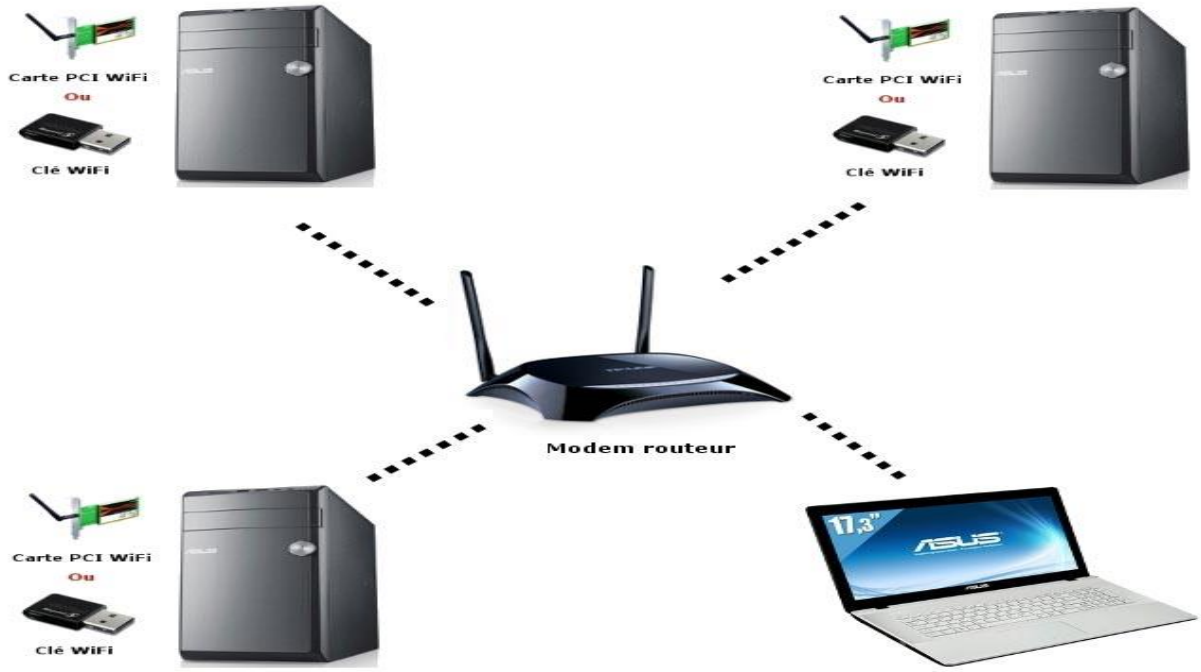


Figure 10 : Modem [5]

II.3.7 La carte réseau : appelée Network Interface Card en anglais est notée NIC, constitue l'interface entre l'ordinateur et le câble du réseau. La fonction d'une carte est de préparer, d'envoyer et de contrôler les données sur le réseau.

La carte réseau possède généralement deux témoins lumineux (LEDs) :

- La LED verte correspond à l'alimentation de la carte
- La LED orange (10 Mb/s) ou rouge (100 Mb/s) indique une activité du réseau (envoi ou réception de données). [2]

Figure 11 : Carte réseau [5]

II.3.8 les serveurs :

Un serveur réseau est un ordinateur spécifique partageant ses ressources avec d'autres ordinateurs appelés clients. Il fournit un service en réponse à une demande d'un client.

Les services rendus par un serveur peuvent être très variés, c'est pourquoi on distingue :

- le serveur de fichiers, qui gère une ou plusieurs bases de données
- le serveur d'impression, qui gère la file d'attente des imprimantes du réseau
- Le serveur d'application.
- le serveur web, qui met à disposition les pages d'un site web (ou intranet) et tout ce qu'elles contiennent
- le serveur de messagerie, qui stocke les messages entrant, et les tient à disposition des ordinateurs clients
- les serveurs propres à Internet : ftp, proxy, DNS, etc. [2]

Figure 12 : Un serveur [5]

II.3.9 Baie de stockage:

Une baie de stockage est un équipement de sauvegarde de données informatique. Bien que son apparence varie souvent, suivant sa taille et son utilisation, sa structure est toujours la même. On retrouve plusieurs éléments, indispensables à son fonctionnement. Elle comporte une série de disques de stockage, qui sont chargés d'emmagasiner les données. La taille de la baie de disque dépend bien évidemment, de la quantité à stocker. [6]

II.3.10 Centre de donnée « DATA CENTER » :

Un centre de donnée ou data center est un site physique sur lequel se trouvent regroupés des équipements constituants du système d'information de l'entreprise (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.). Il peut être interne et/ou externe à l'entreprise. C'est un service généralement utilisé pour remplir une mission critique relative à l'informatique et à la télématique, Il comprend en général un contrôle sur l'environnement (climatisation, système de prévention contre l'incendie, etc.), une alimentation d'urgence et redondante, ainsi qu'une sécurité physique élevée. [2]

Figure 13 : Data Center [5]

II.4 Le modèle TCP/IP (Transport Control Protocol/Internet Protocol) :

Le modèle TCP/IP s'inspire du modèle OSI auquel il reprend l'approche modulaire mais réduit le nombre à quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application. Ce n'est pas le cas du modèle TCP/IP. C'est actuellement le modèle théorique le plus utilisé. [1]

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches

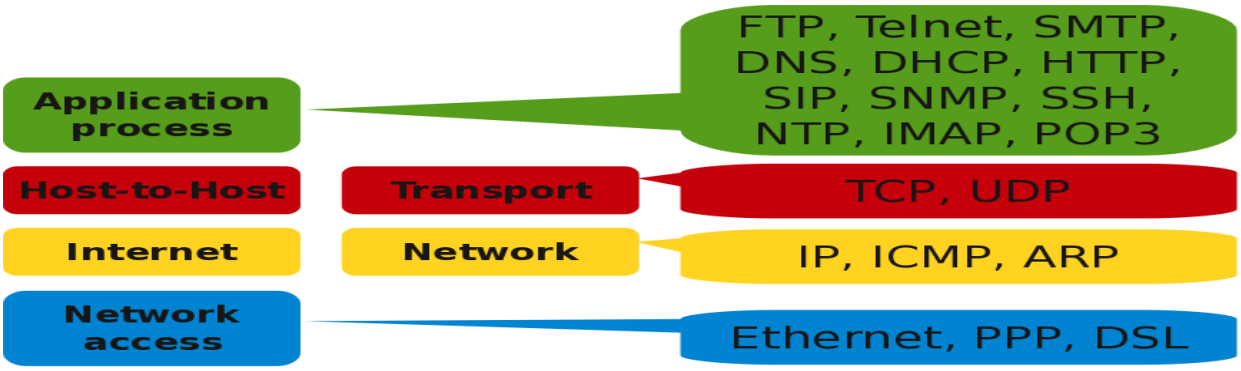


FIGURE 14 : présentation du modèle TCP/IP [5]

- **Couche 1 : couche accès réseau :**

La couche d'accès réseau a pour rôle de transmettre les données sur le média physique utilisé. En fonction du type de réseau, des protocoles différents peuvent être utilisés à ce niveau.

- **Couche 2 : couche Internet :**

Elle permet l'acheminement des datagrammes vers des machines distantes. Elle gère aussi la circulation des paquets à travers le réseau en assurant leur routage, cette circulation des paquets (datagrammes) est gérée par le protocole IP.

- **Couche3 : couche transport (Host-to-Host) :**

La couche transport prend en charge la gestion de connexion, le contrôle de flux, la retransmission des données perdues et d'autres modes de gestion de flux. Les protocoles TCP et UDP sont dédiés à ces fonctions de transport.

- **Couche 4 : couche application**

La couche application sert à l'exécution des protocoles de niveau utilisateur tels que les échanges de courrier électronique (SMTP), le transfert de fichiers (FTP) ou les connexions distantes (Telnet).

II.5 Services et protocoles de communication :

II.5.1 Services réseaux :

Un service réseau est un programme qui exécute une fonction utile dans le réseau. Il existe deux types :

- Services d'infrastructure, qui sont utiles pour le bon fonctionnement de tout le réseau. Par exemple, DHCP, DNS, Authentification, etc…
- Services utilisateurs, qui sont utiles pour certains programmes utilisateur (Proxy Web, Base de données, Serveur de fichiers). [3]

II.5.2 Protocoles de communication :

Dans les réseaux informatiques et de télécommunications, un protocole de communication est la spécification d'un ensemble de règles qui définissent comment deux ordinateurs doivent communiquer. [3]

Conclusion partielle :

Dans ce deuxième chapitre, nous avons présenté et su défini le réseau, ses éléments d'interconnexion, ses topologies, les protocoles de communication, ainsi que les différentes méthodes et façons dont les réseaux sont liés. Grâce à cette partie théorique, nous sommes arrivés à comprendre et se familiariser avec les concepts utilisés dans les différents réseaux.

Introduction :

La disponibilité constante d'un système informatique demeure cruciale pour toute entreprise dont la capacité de production repose sur son système informatique. Disposer d'un système fiable, disponible en tout temps est donc capital pour la pérennité des activités d'une entreprise.

Pourtant, même avec du matériel performant, personne n'est à l'abri d'une panne, car d'innombrables paramètres (température du local technique, serveur saturé, etc.) peuvent entrainer des défaillances se traduisant rapidement par une indisponibilité du système.

III.1 Définition du monitoring :

Le monitoring se définit comme une technique utilisant des ressources informatiques pour obtenir des informations sur l'état des réseaux et de leurs composants. Ces données seront traitées et affichées afin de mettre en lumière d'éventuels problèmes. La supervision peut résoudre les problèmes automatiquement ou dans le cas contraire prévenir les administrateurs via un système d'alerte (email ou SMS par exemple). Plusieurs actions sont ainsi réalisées : Acquisition de données, analyse, puis visualisation et réaction.[7]

Figure 15 : Différents interfaces des outils du monitoring [13]

Un tel processus est réalisé à plusieurs niveaux d'un parc de machines : Au niveau interconnexions (Réseau), au niveau de la machine elle-même (Système) et au niveau des services offerts par cette machine (Applications).

III.1.1 Supervision réseau :

Le rôle de la supervision réseau est de s'assurer du bon fonctionnement des communications et de la performance des liens (débit, latence, taux d'erreurs). C'est dans ce cadre que l'on va vérifier par exemple si une adresse IP est toujours joignable, ou si tel port est ouvert sur telle machine, ou faire des statistiques sur la latence du lien réseau.

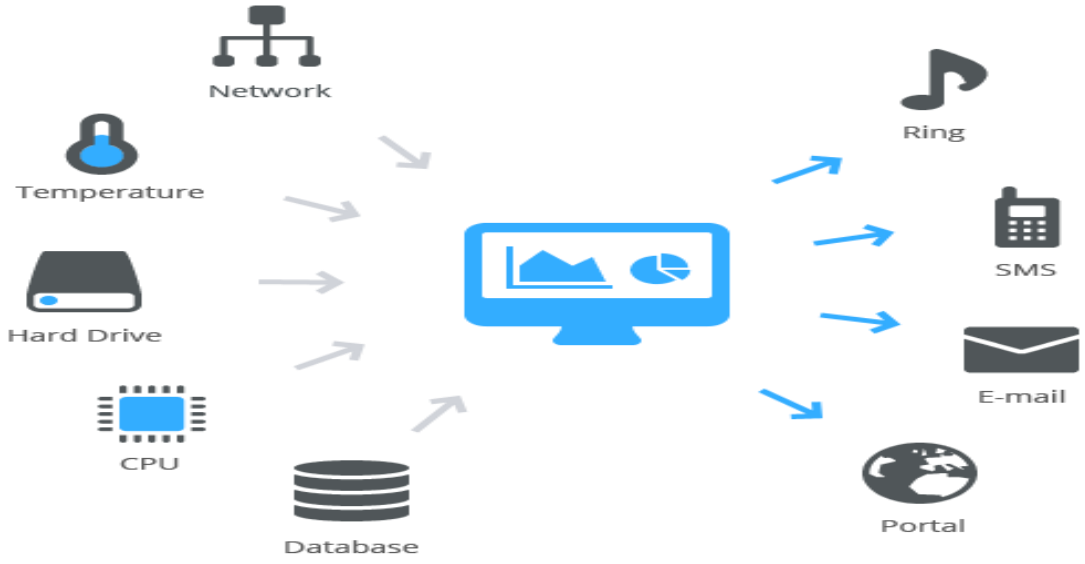


Figure 16 : Supervision réseau [15]

III.1.2 Supervision système :

La surveillance dans ce cas est au niveau de la machine elle-même et en particulier ses ressources. Si l'on souhaite par exemple contrôler la mémoire utilisée ou la charge du processeur sur le serveur.

Figure 17 : Supervision système [16]

III.1.3 Supervision applicative :

C'est une technique qui permet de vérifier le bon fonctionnement d'une application lancée sur une machine. Par exemple une tentative de connexion sur le port de l'application pour voir si elle retourne ou demande bien les bonnes informations, mais aussi de l'analyse de logs applicatifs.

Figure 18 : supervision applicative [16]

III.2 Les différents outils du monitoring :

Dans cette partie nous allons présenter les principaux outils de supervision réseau open source que nous avons choisi vu la diversité de ces outils :

III.2.1 Cacti :

C'est un logiciel de supervision réseau basé sur RRDTool. Il permet de représenter graphiquement divers statuts de périphériques réseau utilisant SNMP ou encore grâce à des scripts (Bash, PHP, Perl,…) pour avoir par exemple l'espace disque restant ou bien la mémoire utilisée, la charge processeur ou le ping d'un élément actif. Les données sont récoltes auprès des différents agents SNMP (ou auprès des scripts locaux) grâce à un script PHP. Pour de meilleures performances un exécutable, nommé cactid, peut également effectuer les interrogations. [8]

III.2.2 Zabbix :

Zabbix est un outil de supervision, concurrent de Nagios et MRTG. Il permet de superviser le réseau et les systèmes (processeur, disque, mémoire, processus,…). Zabbix offre des vues graphiques (générés par RRDtool) et des alertes sur seuil. Le « serveur ZABBIX » peut être décomposé en 3 parties séparées : Le serveur de données, l'interface de gestion et le serveur de traitement. Chacune d'elles peut être disposée sur une machine différente pour répartir la charge et optimiser les performances. Un agent ZABBIX peut aussi être installé sur les hôtes Linux, UNIX et Windows afin d'obtenir des statistiques comme la charge CPU, l'utilisation du réseau, l'espace disque… Le logiciel peut réaliser le monitoring via SNMP. Il est possible de configurer des « proxy Zabbix » afin de répartir la charge ou d'assurer une meilleure disponibilité de service. [8]

III.2.3 Nagios :

Nagios est un logiciel qui permet de superviser un système d'information. Il est, avant toute chose, un moteur gérant l'ordonnancement des vérifications, ainsi que les actions à prendre sur incidents (alertes, escalades, prise d'action corrective). L'interface web est la partie graphique visible, via un serveur web tel que Apache, et qui va permettre à l'administrateur d'avoir une vue d'ensemble de son réseau, de visualiser la supervision des équipements et de produire des rapports d'activité. [8]

III.3 Autres petits outils de monitoring :

On ne peut pas réellement parler de supervision, mais quand même de surveillance en utilisant des petits outils simples qui, une fois combinés à l'aide de langages de scripts permettent de réaliser des choses très intéressantes. D'autres part, ces petits outils sont la base

des plus grosses solutions de supervision, il semble donc intéressant d'appréhender leur fonctionnement. [7]

III.3.1 Outils SNMP :

Il existe bien évidemment des programmes simples destinés à utiliser le protocole SNMP. Leurs noms indiquent quelle requête ils peuvent envoyer, par exemple : snmpget, snmpgetnext, snmpinform, snmpset etc…

Chacune de ses commandes permet de réaliser la requête en utilisant une des trois versions du protocole SNMP. Elles sont énormément utilisées dans le cadre de scripts qui stockent les valeurs obtenues afin de réaliser des statistiques ou des alertes.

III.4 Présentation du protocole SNMP et son principe de fonctionnement :

Pour introduire le protocole SNMP, il faut se rappeler que l'informatique est de plus en plus présente dans notre vie de tous les jours. On compte désormais sur les services offerts par les réseaux pour le fonctionnement de l'outil informatique, que ce soit en entreprise, lors de transactions bancaires, lors de téléconférences, etc. [9]

Pour assurer que ces services soient convenables, il est nécessaire de surveiller le réseau et d'agir quand une erreur se produit.

III.4.1 Définition :

SNMP (Simple Network Management Protocol) est un protocole relativement simple, qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance .Actuellement le plus utilisé pour la gestion des équipements de réseaux grâce à la puissance de ses fonctionnalités qui permet la gestion des réseaux hétérogènes complexes.

III.4.2 Architecture :

Les différents éléments que l'on peut identifier avec le protocole SNMP :

- Les agents SNMP : ce sont les équipements (réseau ou serveur) qu'il faut superviser.
- Le superviseur SNMP : c'est une machine centrale à partir de laquelle un opérateur humain peut superviser en temps réel toute son infrastructure, diagnostiquer les problèmes et finalement faire intervenir un technicien pour les résoudre.

- La MIB : ce sont les informations dynamiques instanciées par les différents agents SNMP et remontées en temps réel au superviseur.
- Les outils SNMP : Ce sont les différents utilitaires utilisés par le superviseur pour l'aider à diagnostiquer un problème. Ces différents outils sont aussi utilisés lors de la configuration du superviseur pour prendre en compte les spécificités de l'infrastructure.

La figure ci-dessous synthétise ces éléments :

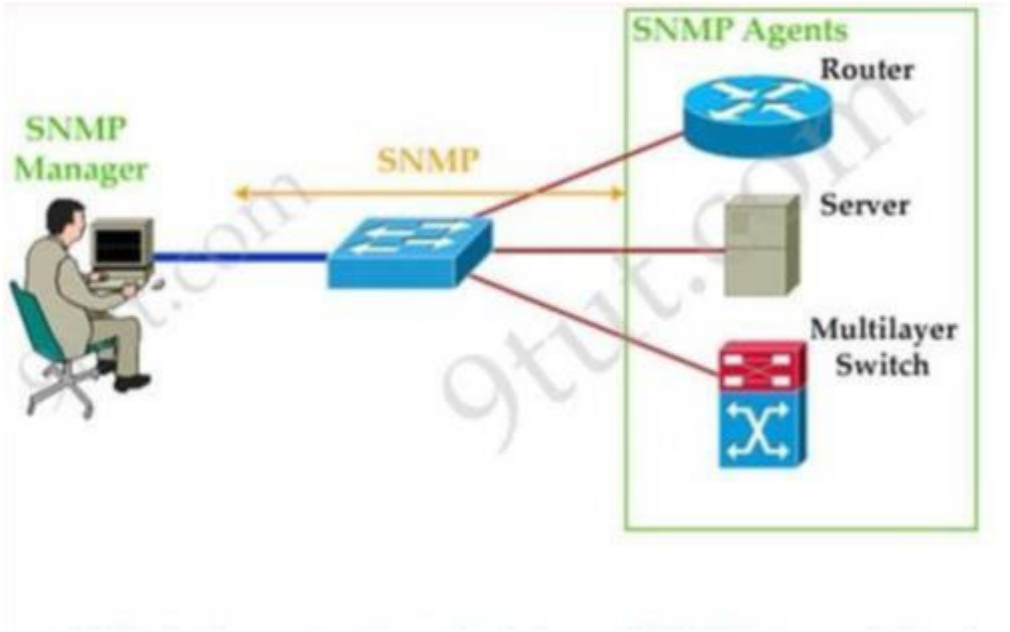


Figure 19 : Architecture SNMP [9]

III.4.3 Fonctionnement :

Le protocole SNMP est constitué d'un ensemble de requêtes, de réponses et d'alertes. Il est basé sur un fonctionnement asymétrique. Le manager envoie des requêtes à l'agent, lequel renvoie des réponses. Lorsqu'un événement inhabituel surgit, l'agent envoie une alerte (trap) au manager. [9]

SNMP utilise le protocole UDP .Le port 161 est utilisé par l'agent pour recevoir les requêtes de la station de gestion. Le port 162 est réservé pour la station de gestion pour recevoir les alertes des agents

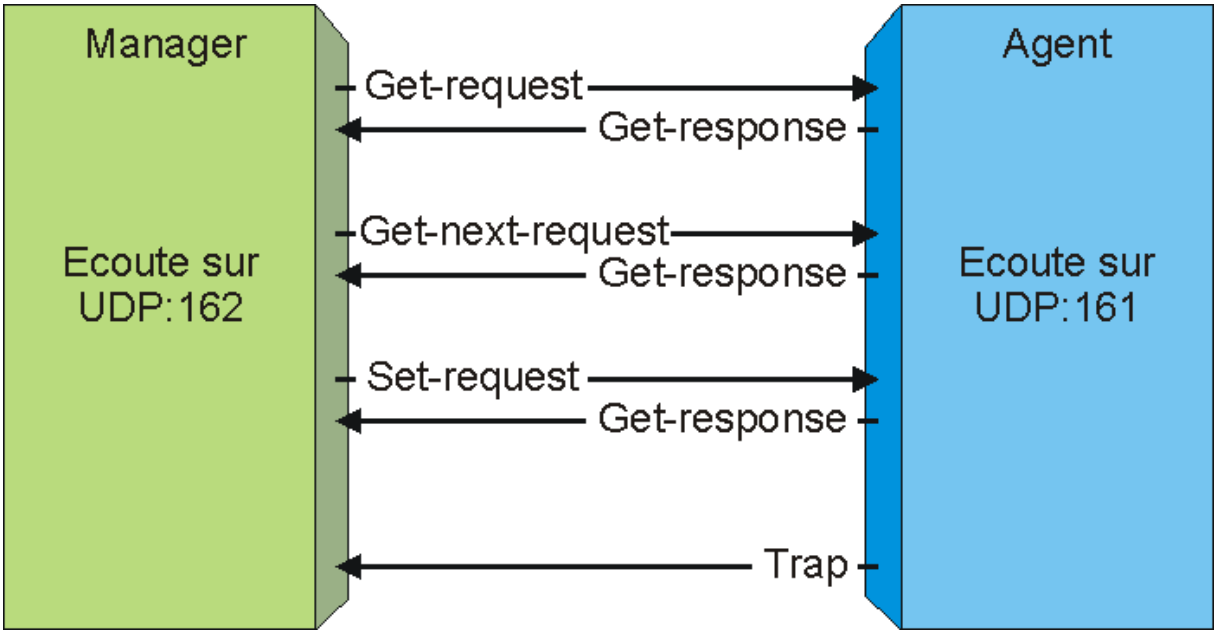


Figure 20 : Fonctionnement du SNMP [14]

- **Les requêtes SNMP :**

Il existe quatre types de requêtes :

- ✓ La requête GetRequest : permet la recherche d'une variable sur un agent.
- ✓ La requête GetNextRequest : permet la recherche de la variable suivante.
- ✓ La requête GetBulk : permet la recherche d'un ensemble de variables regroupées.
- ✓ La requête SetRequest : permet de changer la valeur d'une variable sur un agent.

- **Les réponses de SNMP :**

À la suite de requêtes, l'agent répond toujours par GetResponse. Toutefois si la variable demandée n'est pas disponible, le GetResponse sera accompagné d'une erreur noSuchObject.

- **Les alertes (Traps, Notifications) :**

Les alertes sont envoyées quand un événement non attendu se produit sur l'agent. Celui-ci en informant la station de supervision via une trap.

Les alertes possibles sont : ColdStart, WarmStart, LinkDown, LinkUp, Authentification Failure. [9]

III.4.4 Les différentes versions du SNMP :

Depuis la création de SNMP, ce protocole a connu des améliorations importantes. Dans cette partie on va présenter les trois versions principales et actuellement les plus utilisées (par importance d'utilisation). [10]

- SNMP V1 : C'est la première version du protocole. La sécurité de cette version est minimale car elle basée uniquement sur la chaîne de caractère appelée "communauté". Cette version du protocole est définie dans les RFC 1155 et 1157.
- SNMP V3 : Aussi connu sous le nom de version sécurisée de SNMP. Cette version facilite la configuration à distance des entités SNMP. Un support de SNMP V3 a récemment été lancé car il est plus sécurisé si on le compare à ses prédécesseurs.
- SNMP V2C : C'est un protocole révisé, qui comprend les améliorations de

SNMP V1 dans différents domaines tels que les types de paquets, les éléments de structure MIB et les requêtes protocolaires MIB. Cependant ce protocole utilise la structure d'administration de SNMP V1 (à savoir "communauté") d'où le terme SNMP V2C.

III.5 Présentation de l'outil Cisco Prime infrastructure et son principe de fonctionnement :

III.5.1 Définition :

Cisco Prime Infrastructure est une solution de management global en temps réel du réseau d'entreprise Wifi / LAN / WAN, qui permet de simplifier la gestion des réseaux sans fil et câblés. Elle permet aussi la gestion du cycle de vie du réseau et la gestion de la performance des applications.

L'outil Cisco Prime infrastructure offre le provisionnement des jours 0 et 1, ainsi que l'assurance du jour N d'une succursale au centre de données. Grâce à cette vue unique et à ce point de contrôle, nous pourrons bénéficier des avantages de One Management à la fois sur le réseau et sur le calcul.[11]

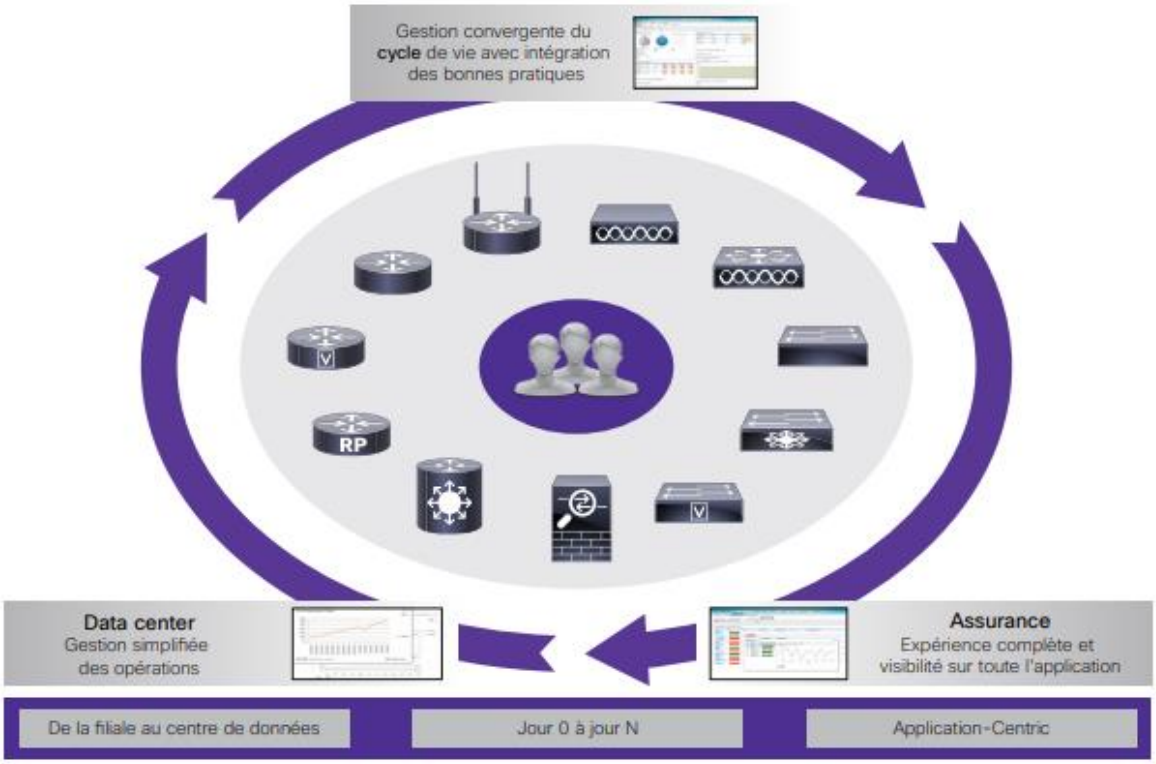


Figure 21 : Plateforme unifié de Cisco Prime Infrastructure [11]

III.5.2 Architecture de Cisco Prime:

L'architecture Cisco Prime fournit une solution de gestion complète pour automatiser la conception, l'exécution, l'assurance et la gestion continue des services réseau avancés tels que la vidéo, la mobilité et les services de cloud gérés sur des réseaux IP.

Elle offre des milliers d'avantages grâce à un cadre flexible de bout en bout des suites Cisco Prime intégrées.

La figure 13 fournit un aperçu de ces suites et de l'architecture Cisco Prime dans son ensemble.

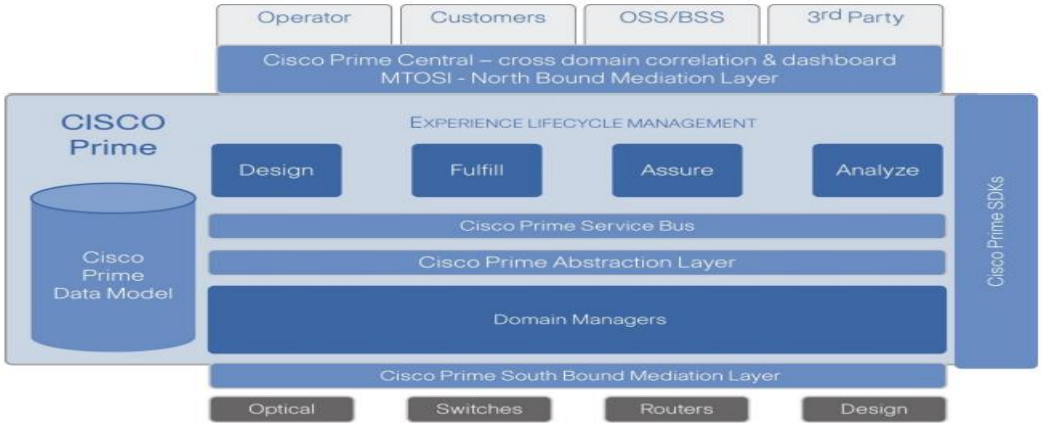


Figure 22 : Présentation d'architecture de Cisco Prime [12]

Explorons chaque composant de l'architecture illustrée ici :

III.5.3 Modèle de données Cisco Prime :

Au cœur de l'architecture, Cisco Prime fournit un modèle de données commun à travers l'infrastructure de bout en bout sous gestion et l'ensemble des expériences du cycle de vie, du service conception par provisionnement et tous les aspects de la gestion et de l'optimisation.

Le modèle de données Cisco Prime est composé de gestionnaires d'éléments (domaines) et basé sur la norme industrielle MTOSI (Multi-Technology Operations Systems Interface) 2.0 du Tele Management Forum (TMF)

III.5.4 Bus de service :

Le bus de service coordonne l'activité entre les gestionnaires du cycle de vie (éléments contrôlant la conception, l'exécution, l'assurance et l'analyse), et entre le cycle de vie et le domaine gestionnaire.

III.5.5 Couche d'abstraction :

Ce composant supprime la complexité de la gestion d'une grande variété d'interfaces en faisant abstraction de l'information dans le modèle de données Cisco Prime. La couche d'abstraction assure la médiation des informations stockées dans le modèle de données et elle est disponible pour tous les composants et interfaces de la suite Cisco Prime.

III.5.6 Gestionnaires de domaine :

Les gestionnaires de domaine fournissent des erreurs de base, la configuration, la fonctionnalité de comptabilisation, de performance et de sécurité (FCAPS) pour chaque domaine technologique spécifique.

III.5.7 Interface de médiation Southbound (SBI) :

La couche Cisco Prime SBI fournit une interface commune, médiatisée pour communiquer avec n'importe quel périphérique Cisco. Elle est utilisée dans chaque gestionnaire de domaine pour extraire les subtilités de la communication de l'appareil via différents protocoles (à savoir, SNMP, CLI, XML, CORBA.etc) en utilisant des interfaces standard.

III.5.8 Interfaces de Northbound(NBI) :

Ces interfaces permettent un accès direct aux gestionnaires de cycle de vie et de domaine à la fois par Cisco Prime Central et des produits tiers tels que les systèmes OSS.Elles sont basées sur des normes et disponibles dans un certain nombre de formats, de services Web et de XML natif

Le NBI est également conçu pour une sécurité maximale, utilisant un cryptage de transport et nécessitant un accès authentifié.

III.5.9 Kits de développement logiciel Cisco Prime (SDK) :

Ces SDK offrent aux fournisseurs de services une flexibilité maximale pour personnaliser la solution et l'intégrer facilement dans leur environnement. Ils comprennent des API et de la documentation pour l'accès aux gestionnaires de domaine ainsi que des gestionnaires de cycle de vie pour les interfaces nord et sud.

III.5.10 Cisco Prime Central :

Cisco Prime Central sert à la fois d'opérateur et de portail de gestion. C'est le composant de l'architecture Cisco Prime qui fournit aux utilisateurs une vue unique de tout l'inventaire géré par les différents gestionnaires de domaine, simplifiant la gestion et le provisionnement des services sur l'infrastructure réseau de bout en bout. Il fournit pour chaque élément du cycle de vie une authentification unique et des services de gestion des utilisateurs avec RBAC (Role-Based Access Control).

Il fournit également une interface d'administration facultative pour tous les produits inclus dans la suite qui répond aux tâches de gestion courantes.

III.5.11 Gestionnaire de cycle de vie (Conception, Réalisation, Assure, Analyse) :

Les gestionnaires de cycle de vie se coordonnent les uns avec les autres via le bus de service Cisco Prime et s'appuient sur le modèle commun de données de Cisco pour le contexte de périphérique et de service partagé.

Ces applications fournissent des services de gestion du cycle de vie des expériences de bout en bout dans tous les domaines technologiques. [12]

III.6 Principe de fonctionnement :

Cisco prime infrastructure est une nouvelle stratégie qui se concentre sur 2 éléments :

1. Consolidation : permet de consolider toute les fonctionnalités gérant le réseau dans une même plateforme qui couvrirait :
    - La gestion de l'image du logiciel
    - La gestion de configuration
    - La gestion des pannes
2. Convergence : permet le regroupement du réseau câblé et sans fils dans la même Plateforme et permet également la convergence des aspects de sécurité ainsi que d'un datacenter en une seule plateforme

Cette nouvelle technologie est considérée également comme une solution unique intégrée pour la gestion de cycle de vie de l'accès filaire ou sans fils.

Ce cycle de vie comporte cinq phases : la conception, le déploiement, l'exploitation, la génération de rapports et l'administration. Les détails de chacune de ces phases sont brièvement décrits dans la section suivante.

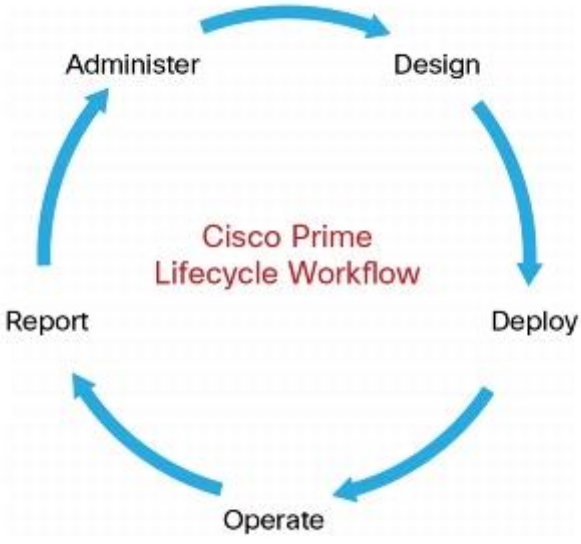


Figure 23 : Flux de travail opérationnel de cycle de vie [11]

- Conception

Au cours de cette phase, on peut évaluer, planifier et créer les configurations requises pour déployer de nouveaux services et technologies réseau. On peut également créer des modèles utilisés pour surveiller les ressources, les périphériques et les attributs clés du réseau.

- Déployer

Dans cette phase, on peut planifier le déploiement et la mise en œuvre des modifications du réseau. Les modifications peuvent inclure des modèles créés lors de la phase de conception, des mises à jour d'images logicielles et la prise en charge des modifications ad hoc et des mises à jour de conformité initiées par l'utilisateur. Cela accélère le déploiement du service, minimise les risques d'erreurs et est hautement évolutif.

- L'exploitation :

On peut utiliser des tableaux de bord préconfigurés pour fournir une surveillance à jour de l'état général du réseau. Des workflows en un clic simple améliorent le dépannage et réduisent le temps nécessaire pour résoudre les problèmes de réseau. Les affichages d'alarme unifiés avec des analyses judiciaires détaillées fournissent des informations exploitables et la possibilité d'ouvrir automatiquement les demandes de service avec le centre d'assistance technique de Cisco (TAC).

- Rapport

On peut fournir une grande variété de rapports préconfigurés pour obtenir des informations actualisées sur le réseau, notamment l'inventaire détaillé, la configuration, la conformité, l'audit, la capacité, la fin de la vente, les failles de sécurité et bien d'autres. Les rapports peuvent être planifiés ou exécutés immédiatement, envoyés par e-mail ou enregistrés au format PDF à des fins de visualisation ultérieure.

- Administrer

Dans cette dernière phase, on peut fournir un ensemble de workflows faciles à utiliser qui aident à maintenir la santé de l'application et à maintenir les périphériques, les utilisateurs et le logiciel à jour, permettant au personnel informatique de se concentrer sur d'autres activités importantes.

Cette solution permet aussi la gestion des performances applicatives en simplifiant les aspects complexes pour une identifications et résolution rapide des failles afin d'offrir un meilleur moyen d'évaluation et rentabilité, et cela en passant par deux étapes :

- Diagnostiquer rapidement l'origine des problèmes de performance
- Améliorer considérablement l'efficacité. [11]

Conclusion partielle :

Dans ce troisième chapitre, nous avons défini le concept du monitoring ainsi que ses différents outils, précisément l'outil Cisco Prime infrastructure dont il est le choix effectué à mettre en place.

Dans le chapitre qui suit nous allons passer à la conception et la réalisation de ce dernier au sein de l'entreprise.

Dans ce chapitre, nous présentons, en premier lieu, les exigences du système et du client pour une bonne installation de notre outil.

En second lieu nous décrivons les étapes de l'installation de l'outil Cisco Prime Infrastructure version 2.2 ainsi que celles de la post-installation.

Enfin nous configurons ce dernier en ajoutant les périphériques et leurs informations afin d'identifier le réseau global sur la plateforme de l'infrastructure, que nous allons par la suite surveiller.

IV.1 Les exigences de la mise en place de l'outil Cisco Prime Infrastructure :

IV.1.1 Exigences du système :

Prime Infrastructure est fourni en tant qu'appliance, c'est-à-dire une machine virtuelle (VM) comprenant l'application elle-même et un système d'exploitation Red Hat Linux Enterprise Server 64 bits sécurisé.

Elle dispose de deux options de déploiement : appliance virtuelle et physique. L'appliance virtuelle est empaquetée en tant que fichier OVA (Open Virtualization Archive), qui doit être installé sur un serveur qualifié exécutant VMware ESXi qui utilise vSphere Client ou ESX5.5U2 Client pour gérer la machine virtuelle.

L'installation doit être avec l'une des quatre configurations, chacune optimisée pour une taille de réseau d'entreprise différente.

Tableau 01 : les différentes configurations de l'appliance virtuelle.[11]

Les options	Express	Express plus	Standard	Professionnel
Virtuel CPU (vCPU)	4	8	16	16
Mémoire (DRAM)	12GB	16GB	16GB	24GB
Capacité du disque (HDD)	300GB	600GB	900GB	1200GB
Débit (Disk I/O)	200 MB/s	200 MB/s	200 MB/s	320 MB/s

IV.1.2 Les exigences du client :

Tous les utilisateurs de Prime Infrastructure accèdent à l'appliance à partir d'un navigateur Web client. Le tableau suivant montre tous les navigateurs pris en charge qui peuvent être utilisés pour y'accéder.

Tableau 02 : les différents navigateurs supportés par CPI.[11]

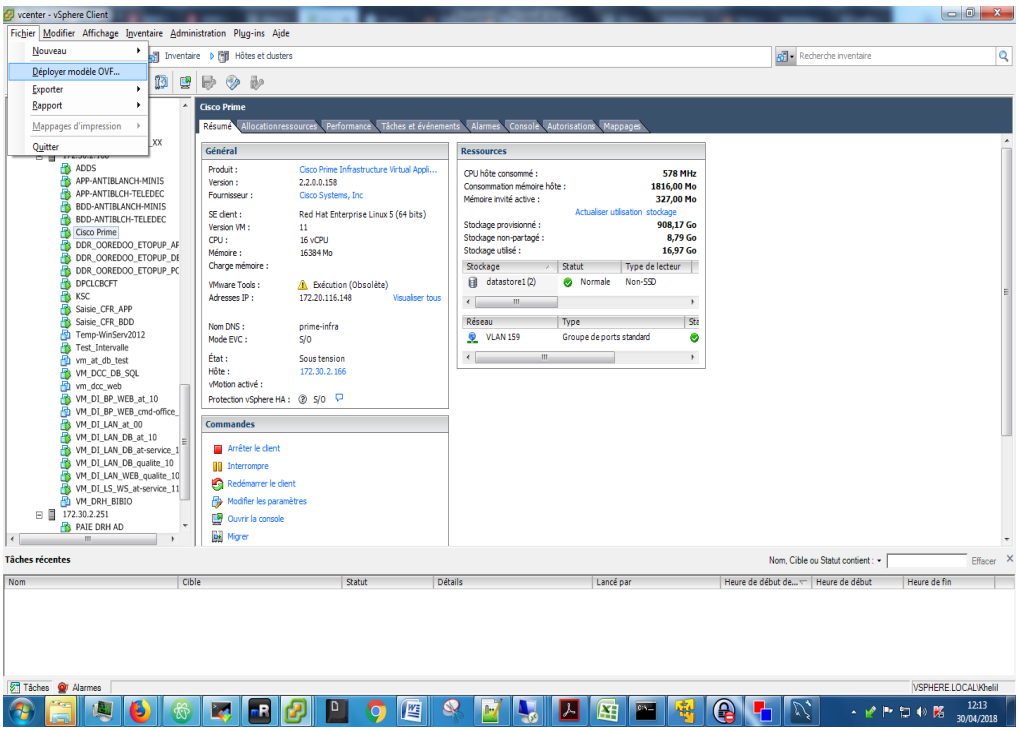
Navigateur pris en charge	Version du navigateur
Internet explorer	10 ou 11
Mozilla Firefox	30
Mozilla Firefox ESR	17, 24
Google Chrome	34, 35, 36

IV.2 Installation de Cisco Prime infrastructure :

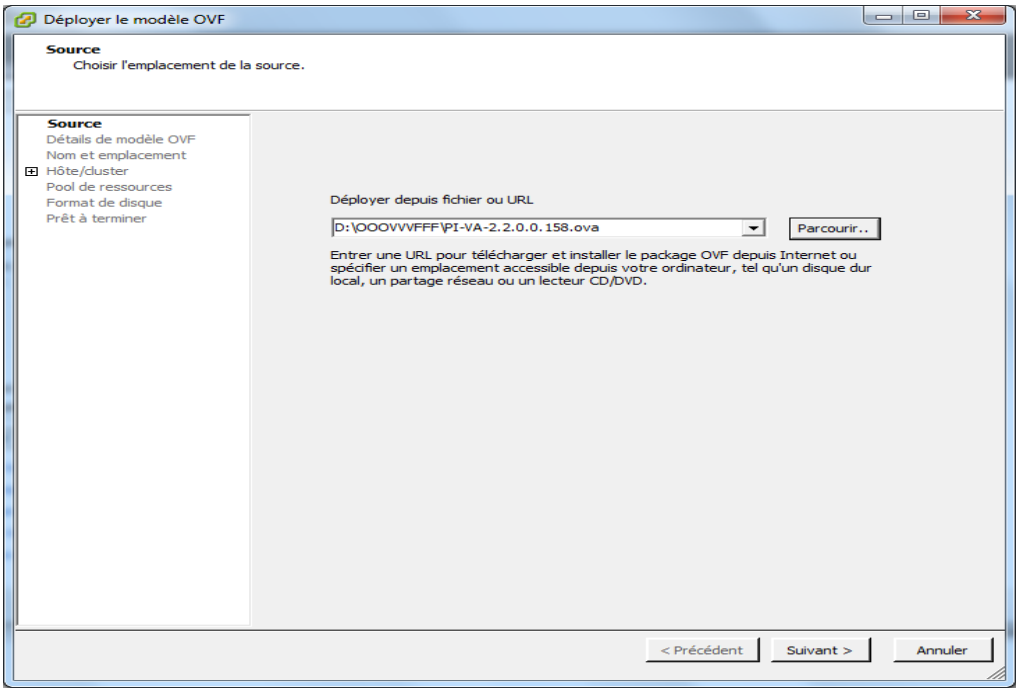
IV.2.1 Déploiement de l'OVA à partir du client VMware vSphere :

Les figures suivantes résument les étapes du déploiement de la version Standard.

Étape 1 : Après avoir lancé la VMware Vsphere client et connecté à l'hôte ESXI on déploie le fichier OVA en choisissant **Fichier>Déployer le modèle OVF,**



Étape 2 : On clique sur **parcourir** pour accéder à l'emplacement où nous avons enregistré le fichier OVA sur notre ordinateur local, puis on clique sur **suivant.**

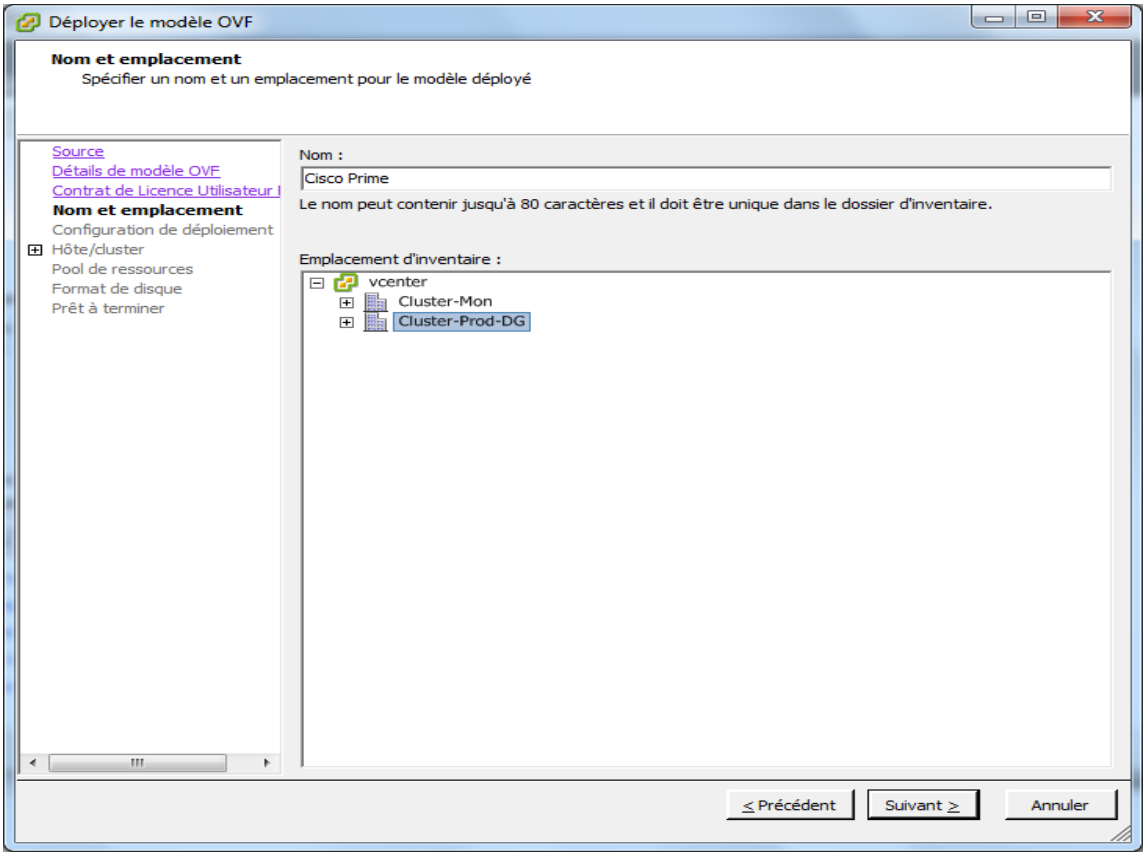


Étape 3 : On vérifie les détails sur la page de détails du modèle OVF, puis on clique sur **suivant.**

Étape 4 : Dans la fenêtre Contrat de licence utilisateur final, on clique sur **Accepter,** puis sur **suivant.**

Étape 5 : Dans la fenêtre Nom et emplacement, on spécifie :

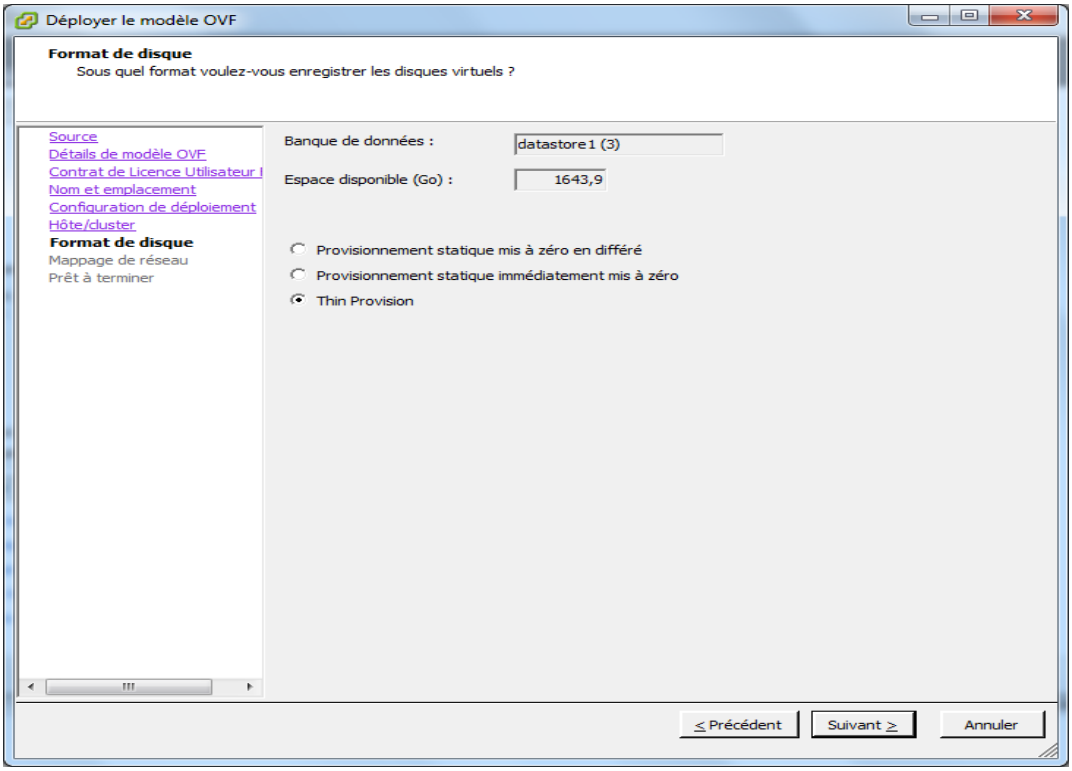
- ✓ Dans le champ Nom : on introduit, le nom de la nouvelle machine virtuelle.
- ✓ Dans la zone Emplacement de l'inventaire : on sélectionne le dossier approprié.



Étape 6 : On clique sur **suivant**

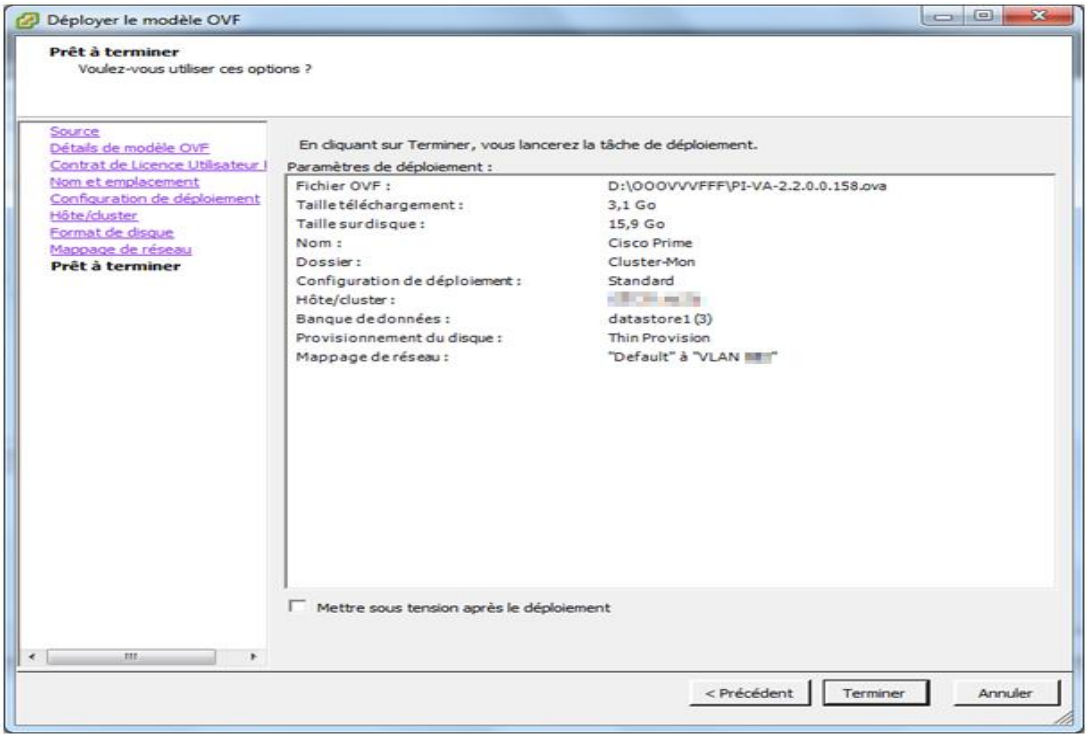
Étape 7 : Dans la fenêtre Configuration du déploiement, on sélectionne la configuration souhaitée (selon les exigences de l'entreprise).

Étape 8 : Dans la fenêtre Format de Disque, on sélectionne Thin Provision.



Étape 9 : Dans la fenêtre Mappage réseau, on sélectionne un réseau utilisé par la machine virtuelle, puis on clique sur Suivant.

Étape 10 : Dans la fenêtre Prêt à terminer, on vérifie nos paramètres, puis on clique sur Terminer.



IV.2.2 Installation du serveur :

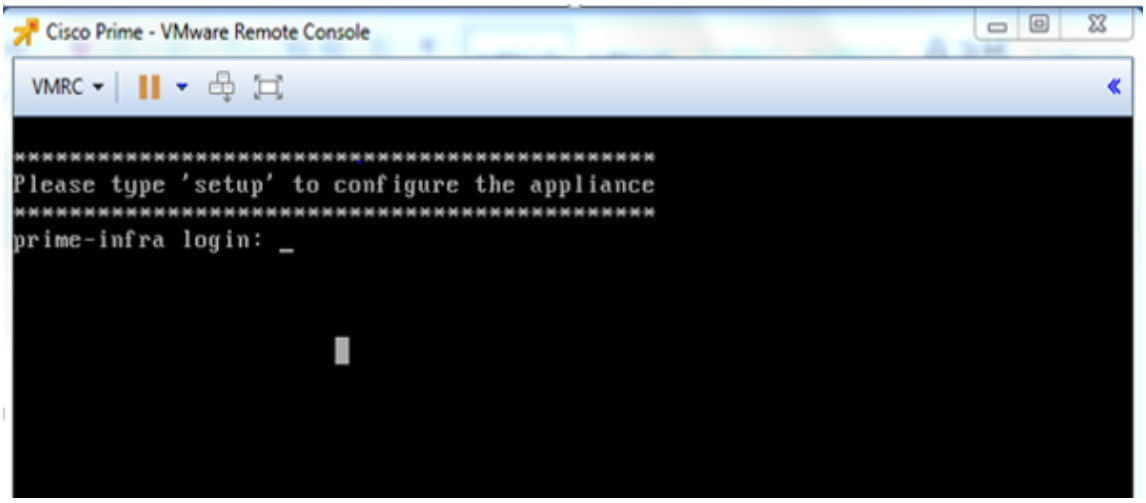
Après le déploiement du fichier OVA, on passe à configuration de l'appliance virtuelle pour l'installation et le démarrage de l'outil.

Les figures suivantes montres les étapes de la configuration.

Étape 1 : Dans la VMware vSphere Client, on clique avec le bouton droit sur l'appliance virtuelle déployée et on choisit Alimentation > Mise sous tension.

Étape 2 : On Clique sur l'onglet Console.

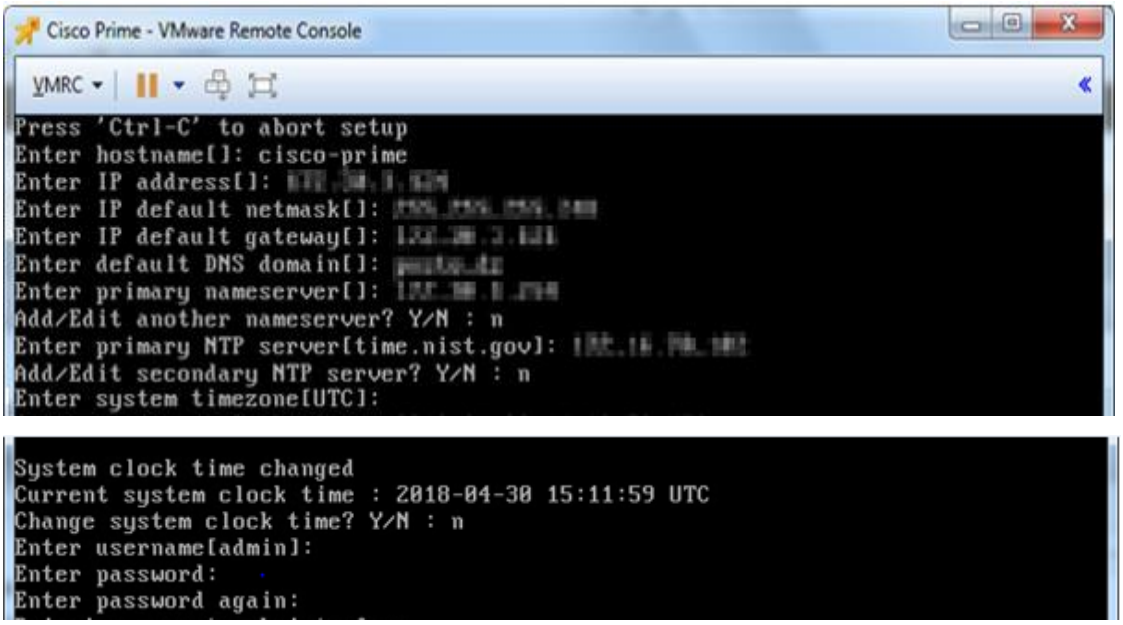
Après le démarrage du serveur, l'invite de connexion localhost s'affiche avec un message en nous demandant de taper « **setup** » pour configurer l'appliance



Étape 3 : La console nous invite à entrer les paramètres suivants:

- ✓ Hostname : nom d'hôte de l'appliance virtuelle.
- ✓ IP Address: adresse IP du dispositif virtuel.
- ✓ IP default netmask : masque de sous-réseau par défaut pour l'adresse IP.
- ✓ IP default gateway : adresse IP de la passerelle par défaut.
- ✓ Default DNS domain : nom de domaine par défaut.
- ✓ Primary nameserver : l'adresse IP du serveur de noms principal.
- ✓ Add/edit another nameserver : la console nous demande si on veut rajouter un autre nom de serveur
- ✓ Primary NTP server : L'adresse IP ou le nom d'hôte du serveur Network Time Protocol principal que nous souhaitons utiliser (time.nist.gov est la valeur par défaut).

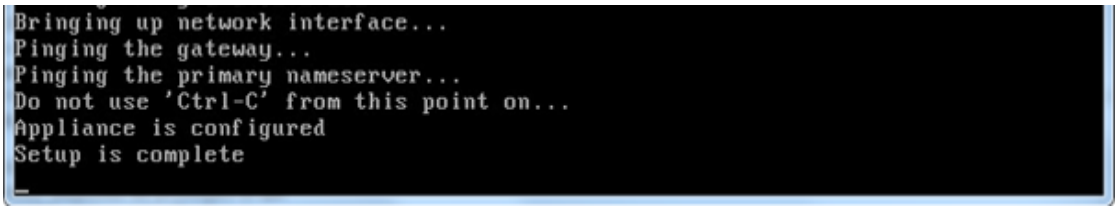
- ✓ Add/Edit Secondary NTP servers : la console nous demande si on veut rajouter des serveurs NTP secondaires à utiliser lorsque le serveur principal n'est pas disponible.
- ✓ Système time-zone [UTC] : le code de fuseau horaire que nous souhaitons utiliser.
- ✓ Current système clock time : la console affichel'heure de l'horloge basée sur le fuseau horaire du serveur, puis nous demande si on veut l'a changé.



- ✓ Username : nom du premier utilisateur administratif (appelé "admin"). C'est le compte administrateur utilisé pour se connecter au serveur via la console ou SSH.
- ✓ Password : le mot de passe de l'administrateur.

Étape 4 : Lorsque nous avons terminé d'entrer ces valeurs, l'application d'installation teste les paramètres de configuration réseau que nous avons entrés.

Si les tests réussissent, l'installation de Prime Infrastructure commence.

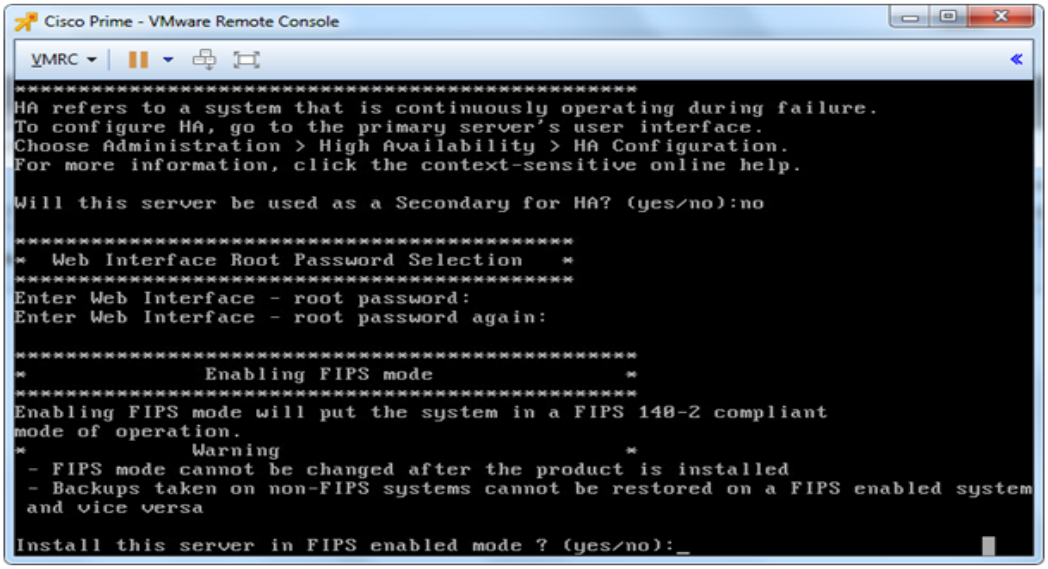


Étape 5 : Une fois l'installation de l'application terminée, les paramètres de post-installation suivants nous seront demandés:

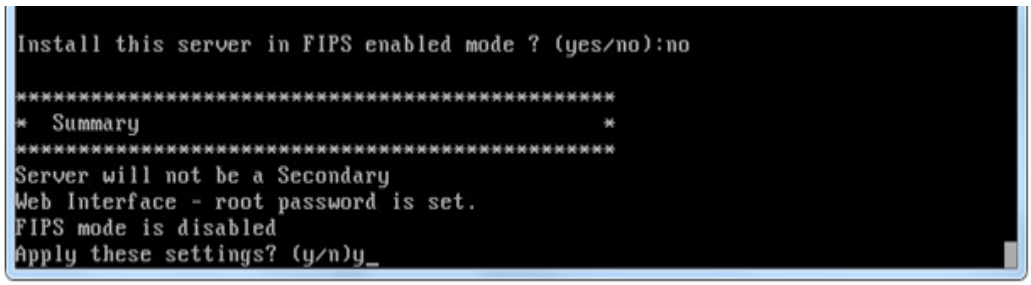
- ✓ High Availability Role Selection : on entre « yes » à l'invite si on souhaite que ce serveur installé serve de serveur secondaire de restauration dans une implémentation de haute disponibilité.

Si on entre « non » à l'invite, le serveur agira en tant que serveur principal (autonome) et l'installation se poursuivra

- ✓ Web Interface RootPassword : on entre et on confirme le mot de passe utilisé pour l'administrateur racine par défaut. C'est le compte utilisé pour se connecter à l'interface utilisateur Web Prime Infrastructure pour la première fois et configurer d'autres comptes d'utilisateurs.



- ✓ Enabling FIPS Mode : On indique « yes » si on souhaite installer Prime Infrastructure dans un mode de fonctionnement conforme FIPS (Federal Information Processing Standards) 140-2. Voir annexe

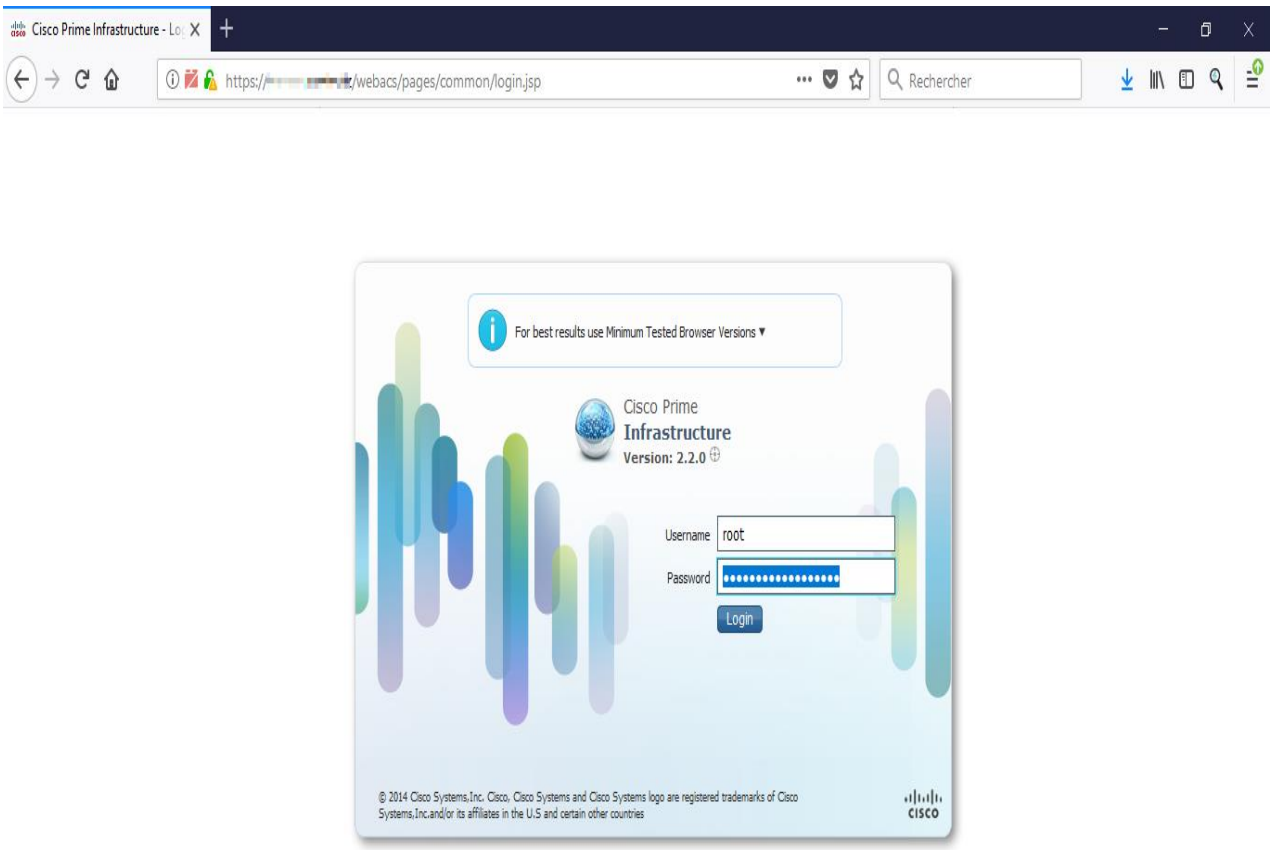


Étape 6 : la console nous affiche un petit résumé de tout ce que nous avons fait et nous demande si on veut appliquer ces paramètres, on répond par « yes »

```
Settings Applied.

Application bundle (NCS) installed successfully

 === Initial Setup for Application: NCS ===

Running database cloning script...
Running database creation script...
_
```

```
INIT: Id "S0" respawning too fast: disabled for 5 minutes
INIT: Id "S0" respawning too fast: disabled for 5 minutes
Setting limits.conf file...
Turning on ipmi service...
Setting up NCS service...
Generating configuration...
Rebooting...
_
```

Étape 7 : Une fois l'installation terminée, l'appliance redémarre et une invite de connexion s'affiche.

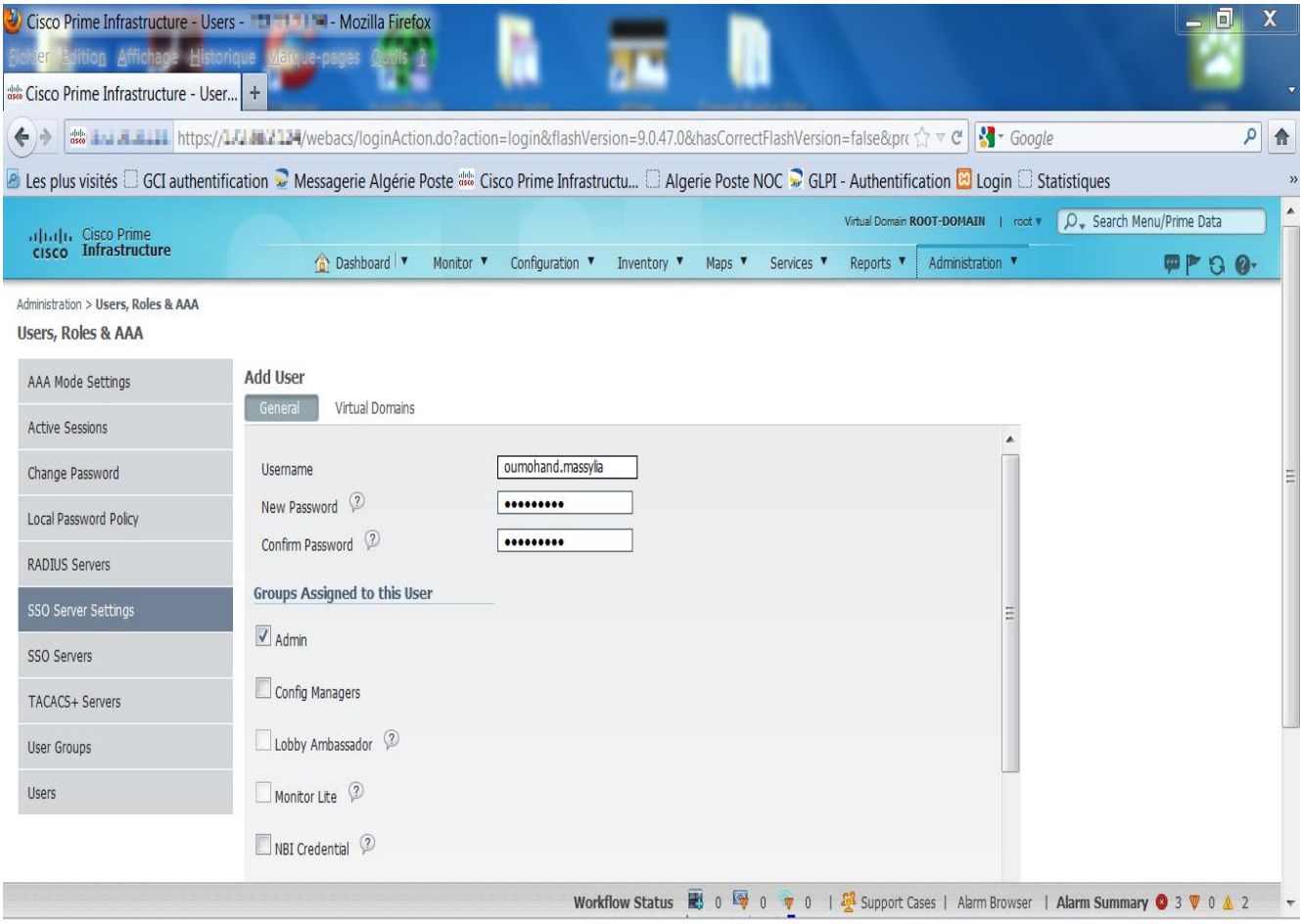


IV.3 Configuration des paramètres et fonctionnalités de Cisco Prime Infrastructure :

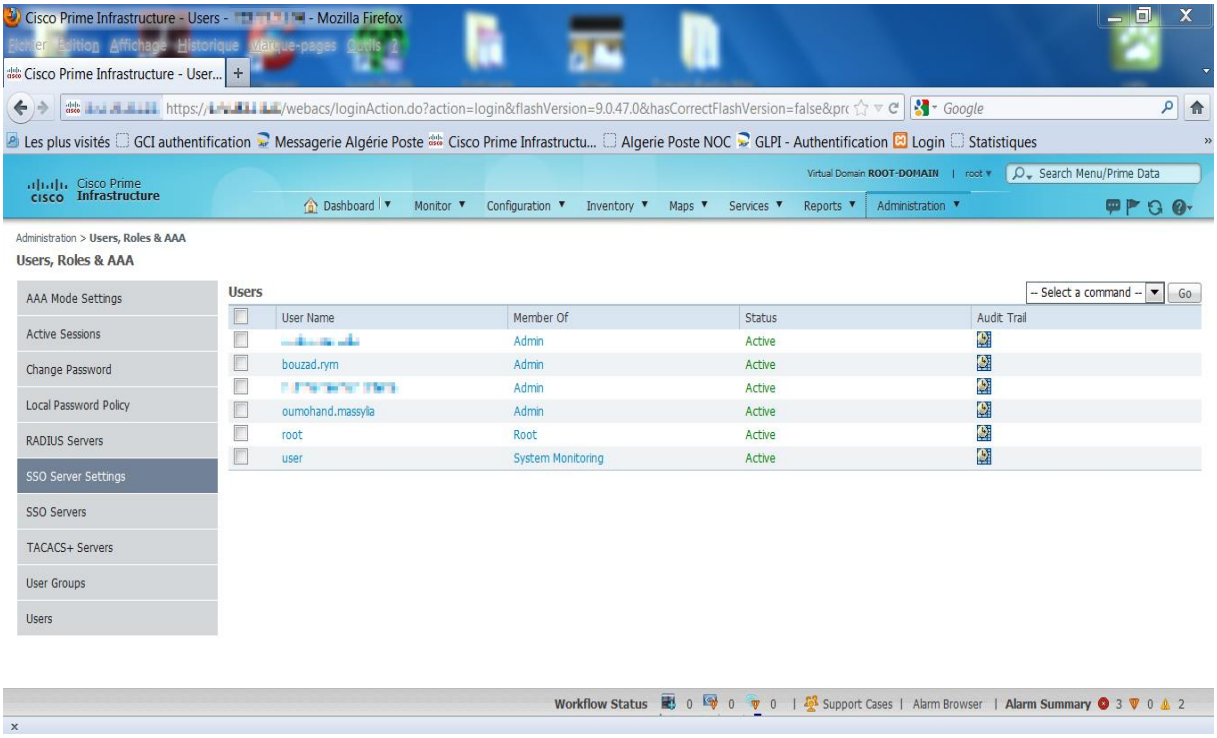
Après s'être connecté sur la plateforme comme utilisateur root, on commence à configurer les différents paramètres dont l'organisme d'accueil a besoin pour gérer le réseau.

IV.3.1 Ajout d'un administrateur :

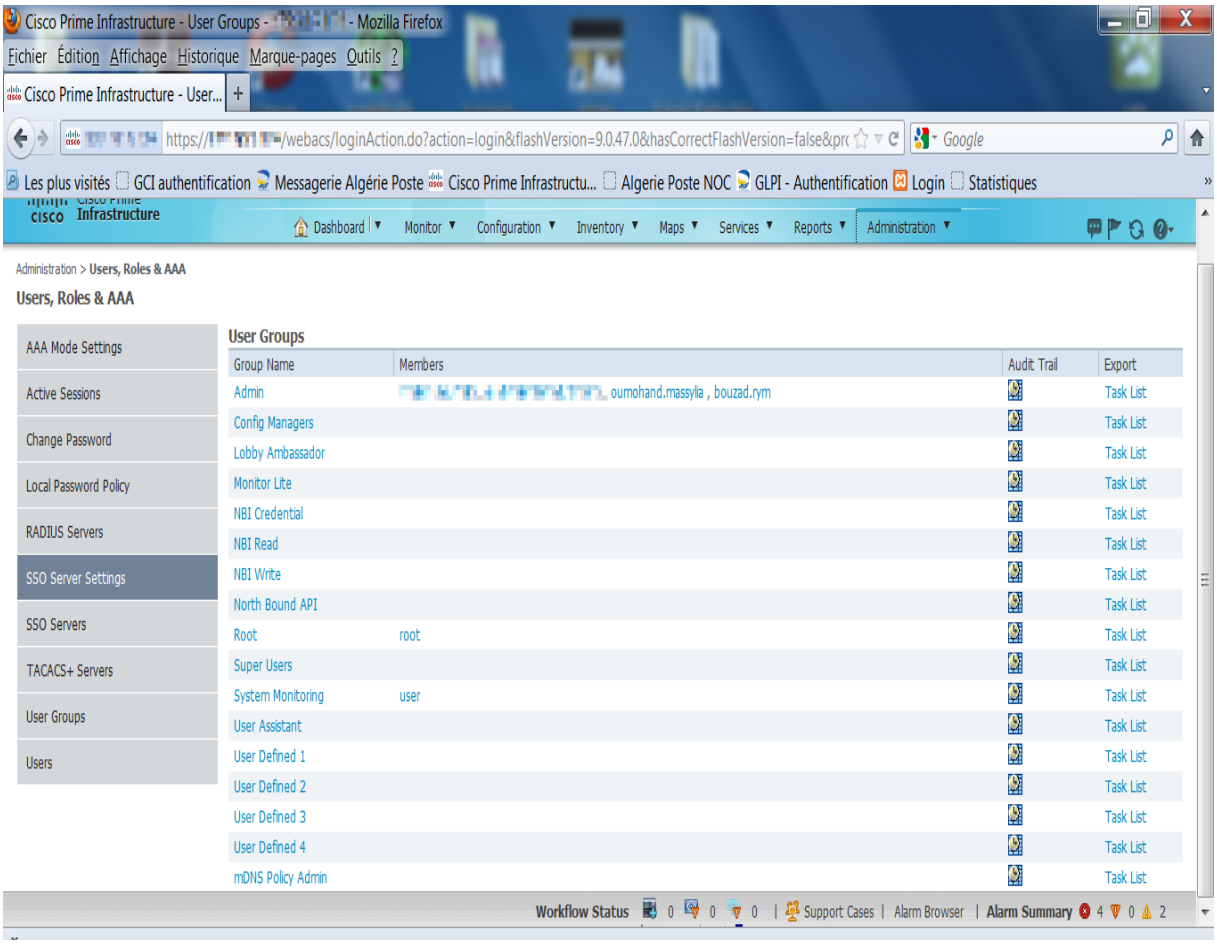
Dans l'onglet **Administration > Users, Roles & AAA**, on clique sur **Add user.** Comme le montre la figure suivante, on introduit le **nom d'utilisateur** ainsi que le **mot de passe.**



La figure qui suit montre les administrateurs existants sur la plateforme ainsi que leurs statuts.



La figure ci-dessous résume les groupes utilisateurs ainsi que leurs membres.

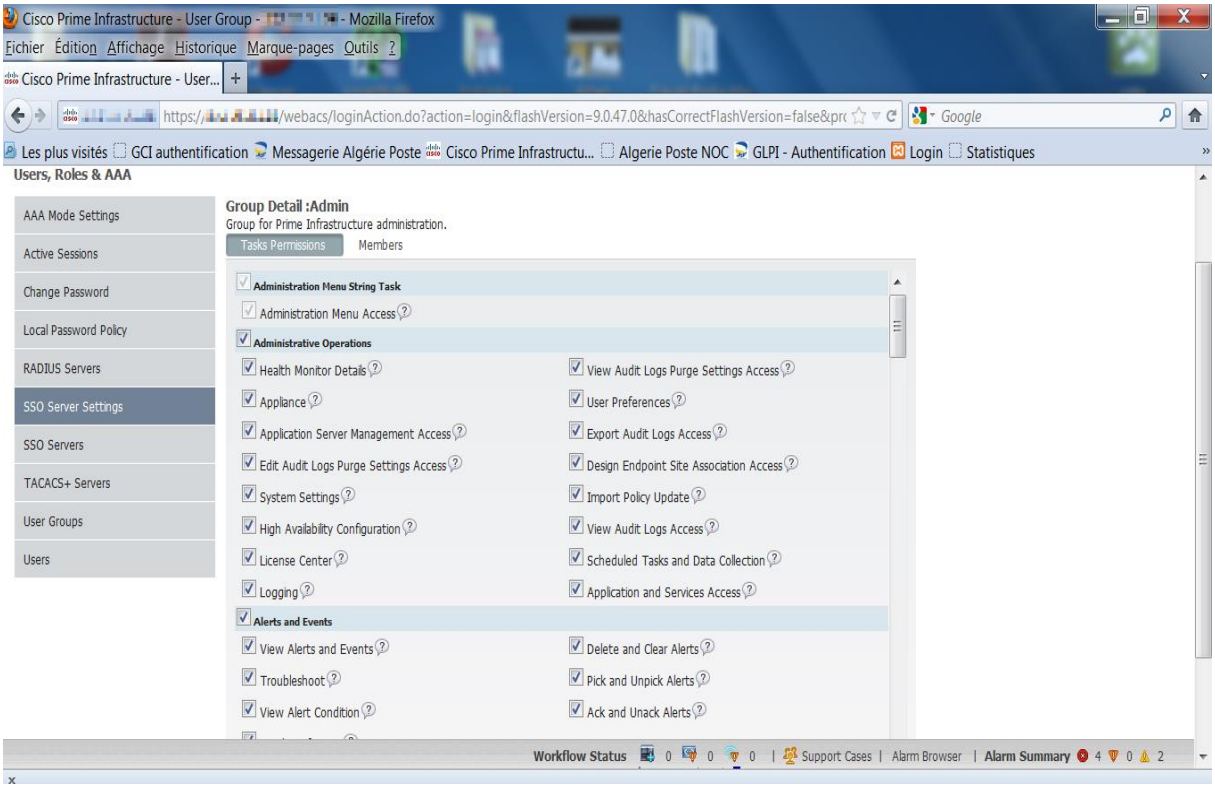


L'utilisateur root peut modifier à tout moment les permissions attribuées à chaque administrateur de Prime Infrastructure.

Explication de quelques permissions :

- **administration string task :** signifiant tâche de chaîne d'administration, qui comprend la permission d'accès au menu d'administration.
- **Administrative operation** signifiant opérations administratives, qui comprend cet ensemble de permissions :
  - détails du moniteur de santé ;
  - détails sur l'appareil ;
  - accès à la gestion du serveur d'applications ;
  - modifier l'accès au paramètre de purge des journaux d'audit ;
  - réglage du système ;
  - configuration à haute disponibilité ;
  - accès au centre de licence ;
  - enregistrement ;
  - afficher les journaux d'audit purger les paramètres d'accès ;
  - préférence de l'utilisateur ;
  - exporter les journaux d'audit ;
  - accès aux associations de sites de terminaux de conception ;
  - mise à jour de la politique d'importation ;
  - tâches planifiées et collecte de données ;
  - l'application et l'accès aux services.

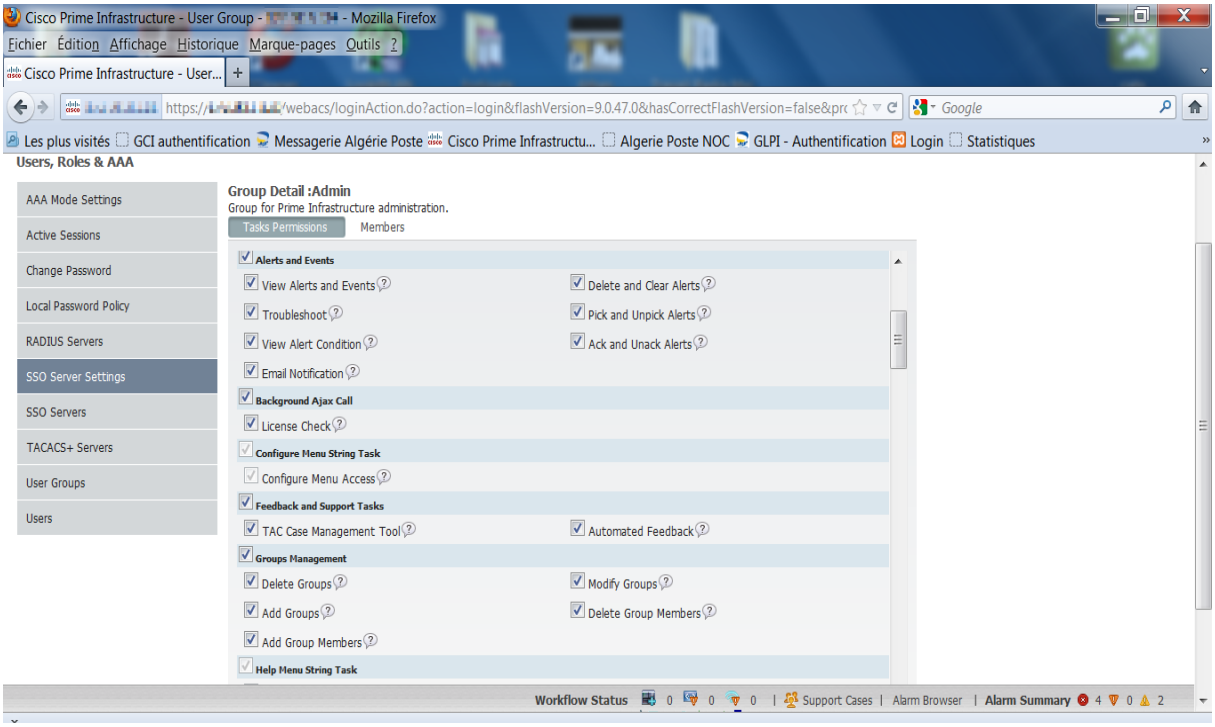
La figure ci-dessous montre ces dernières qu'on peut cocher et décocher sur l'onglet **Tasks Permissions.**



- **alerts and events** signifiant alertes et événements qui comprennent les permissions suivantes :
  - voir les alertes et les événements ;
  - voir la condition d'alerte ;
  - supprimer et effacer les alertes ;
  - choisir et supprimer les alertes
  - recevoir les accusés de réception ;
  - notification par mail ;
  - background ajax call signifie envoyer et récupérer des données depuis un serveur de manière asynchrone (en arrière-plan).
  - vérification de licence ;
- **Configure menu string task** signifie configurer la tache de chaine du menu qui comprend la configuration du menu d'accès.
- **Group management** qui signifie la gestion de groupes comprenant cet ensemble de permissions :
  - supprimer des groupes ;
  - ajouter de groupes ;
  - ajouter un numéro de groupe ;

- modifier les groupes ;
- supprimer les membres du groupes ;

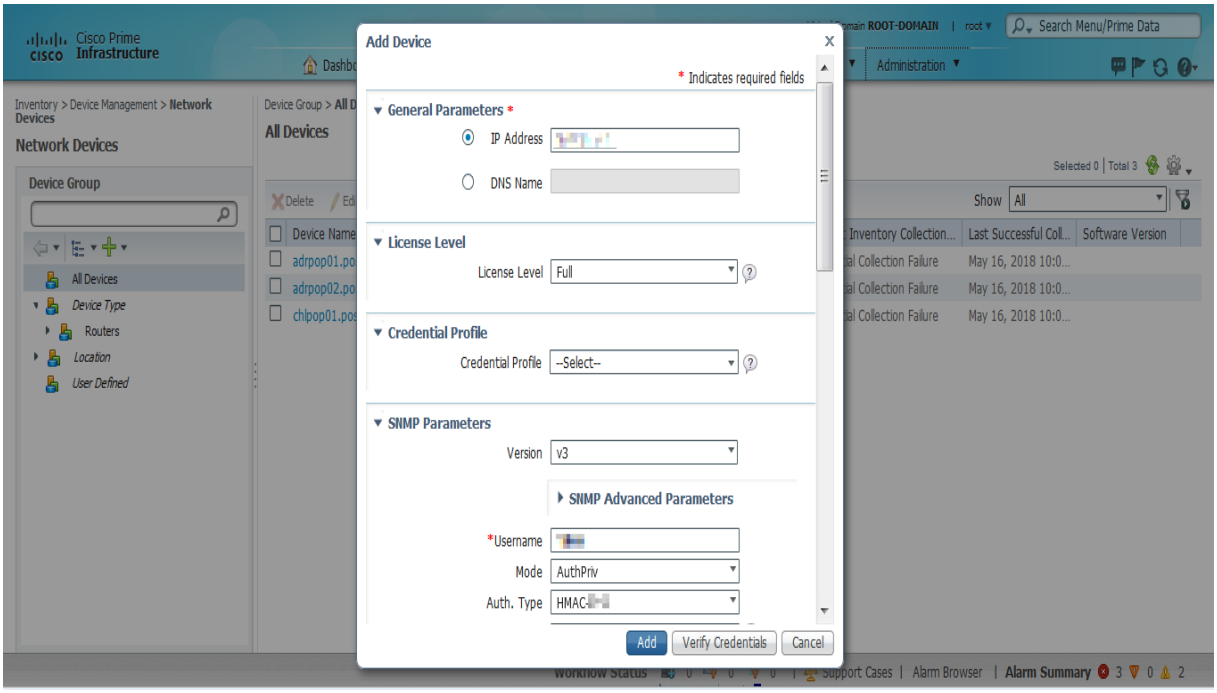
La figure ci-dessous montre les permissions qu'on vient de citer.

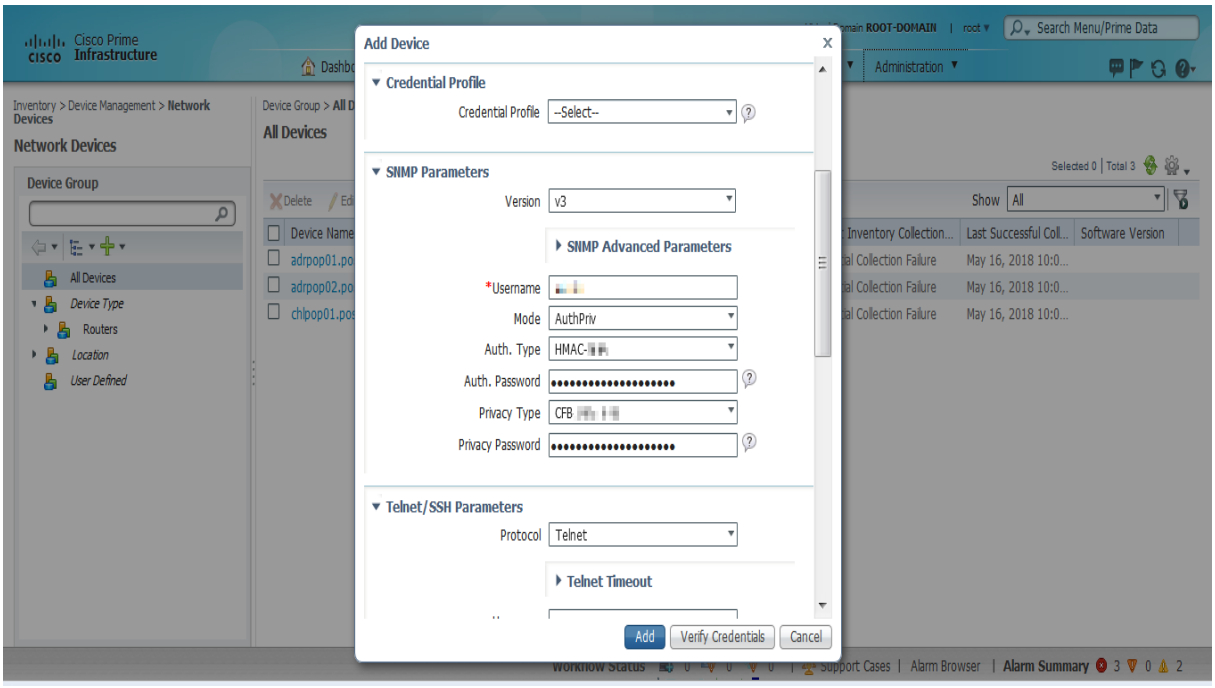


IV.3.2 Ajout d'un périphérique :

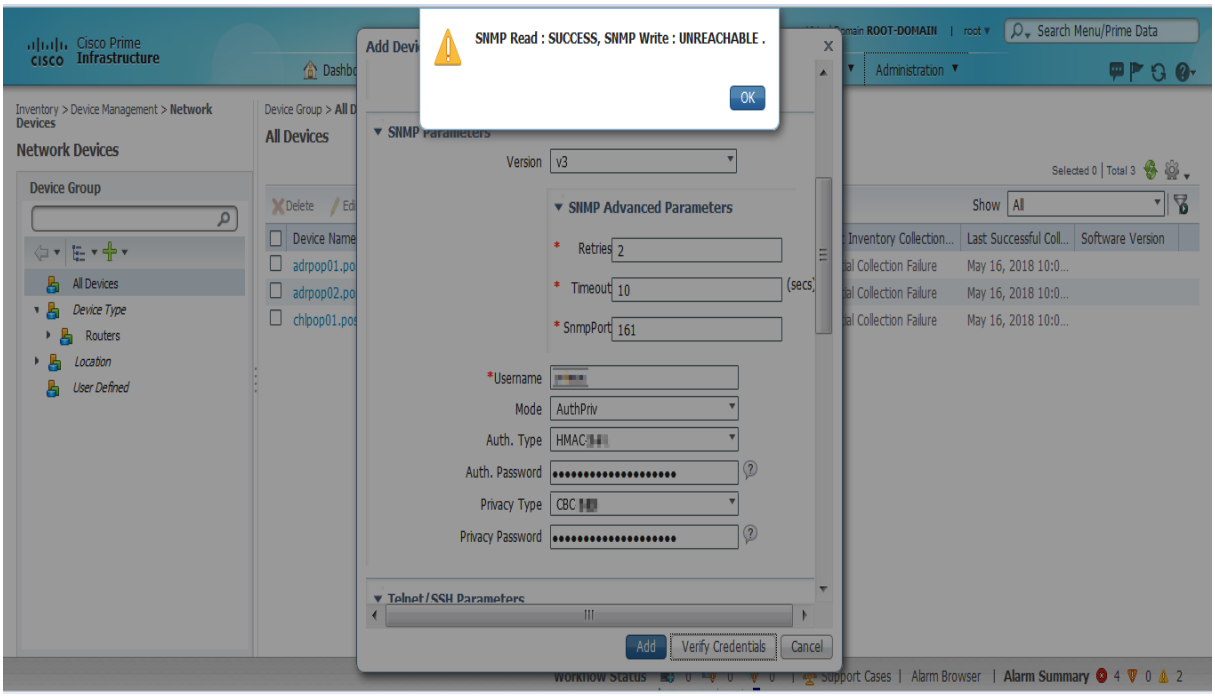
Cet ajout se fait dans l'onglet **Inventory > Device Management > Network Devices**, en suivant ces étapes, en remplissant les champs mentionnés dans les figures ci-dessous et enfin en cliquant sur **Add.**

Dans notre cas on va ajouter le Point de Présence (PoP) de la wilaya de Chlef en entrant son adresse IP et d'autres informations. C'est ainsi que ce périphérique va être reconnu, identifié et par la suite supervisé.

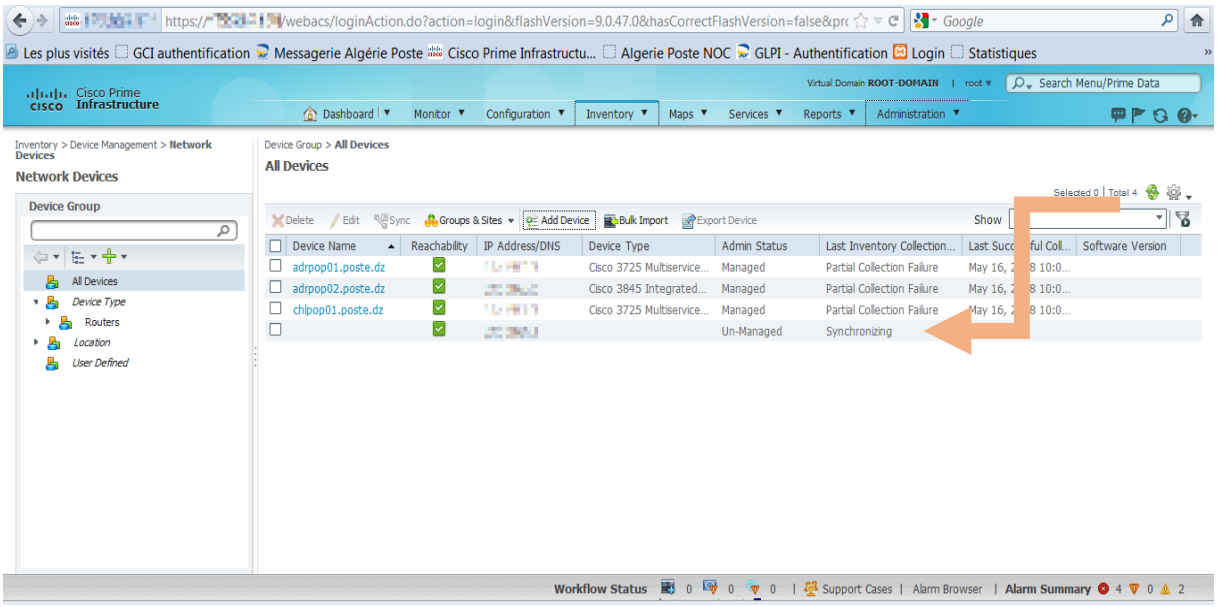


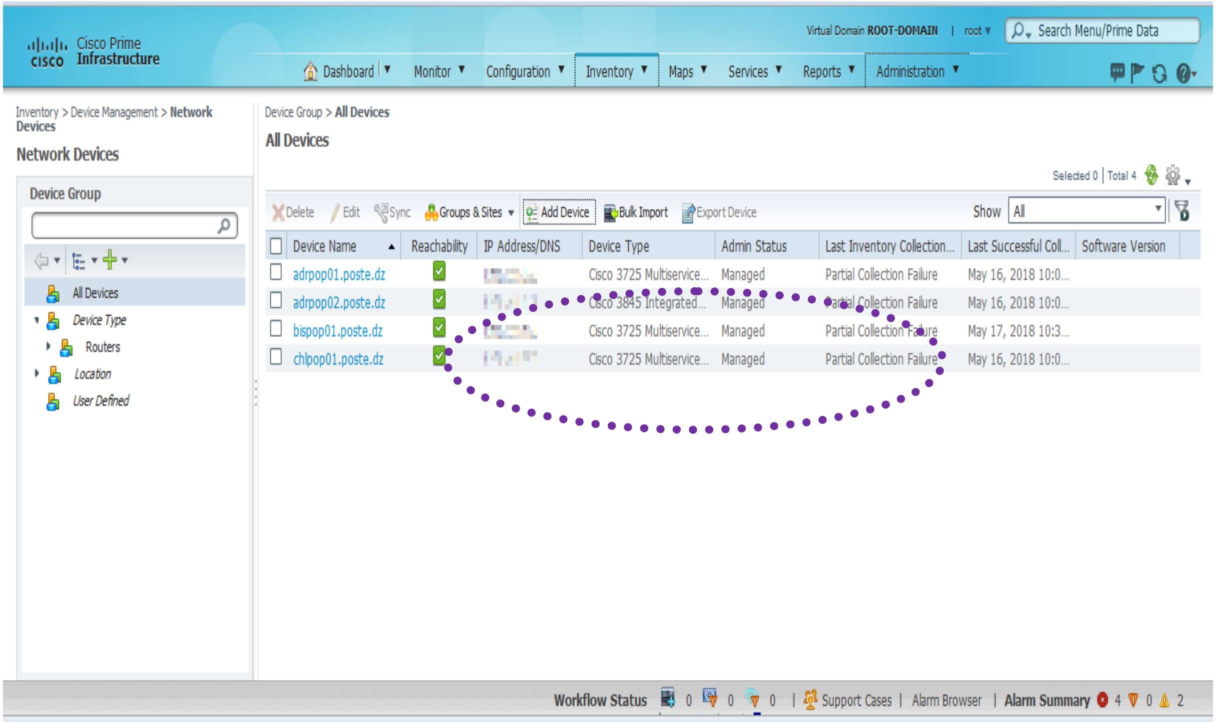


Une fois l'ajout effectué, on reçoit une sorte de notification en haut de la page, telle que celle de la figure ci-dessous.



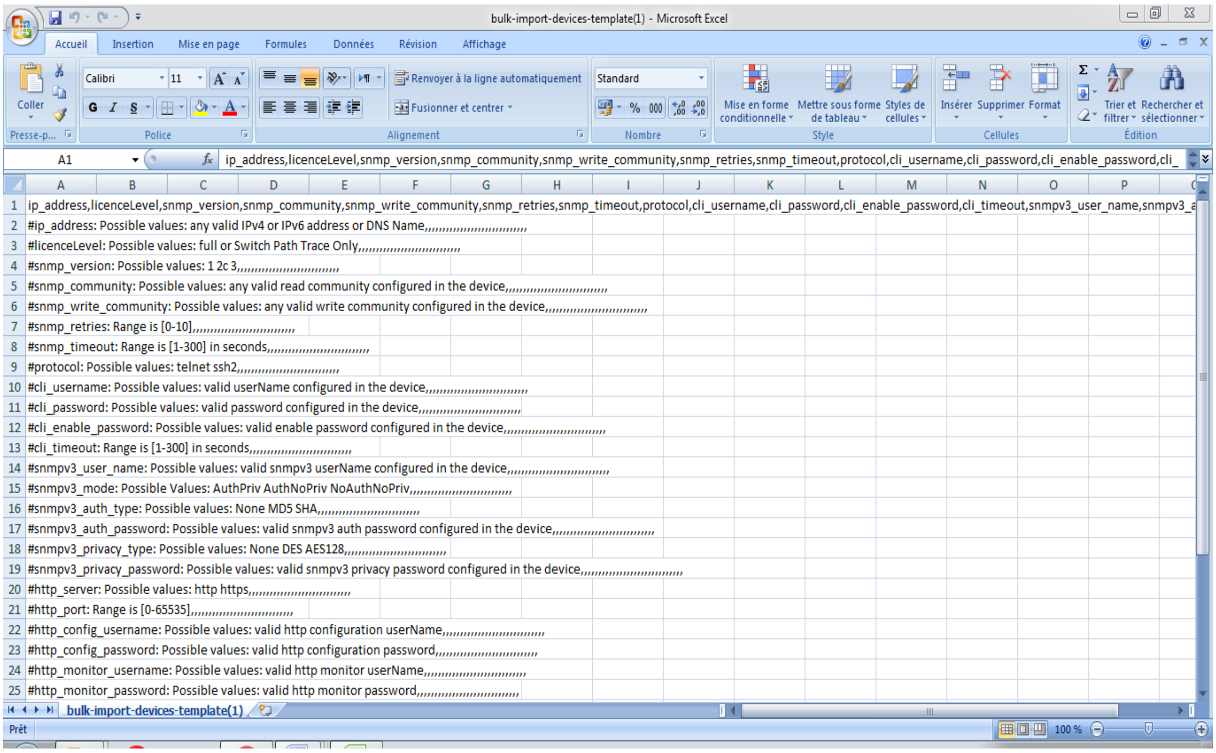
Les figures ci-dessous montrent la synchronisation en cours du PoP Chlef qu'on vient d'ajouter. Puis la mention **managed** qui confirme la fusion ainsi que l'identification de ce PoP d'après son adresse IP.



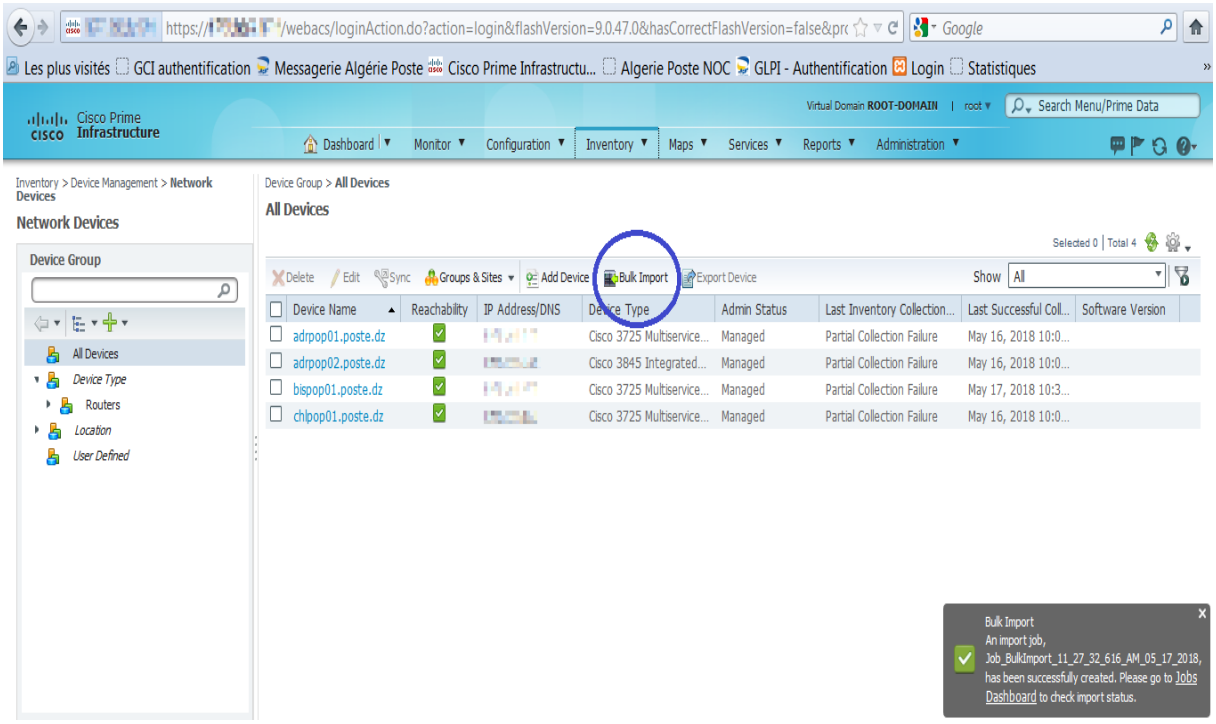


L'ajout des périphériques qu'on vient d'effectuer était un par un. Cependant il existe une fonctionnalité qui regroupe tous les périphériques dans un même fichier d'extension **.CSV**, cela permet de gagner du temps quand on a affaire à des centaines d'équipements.

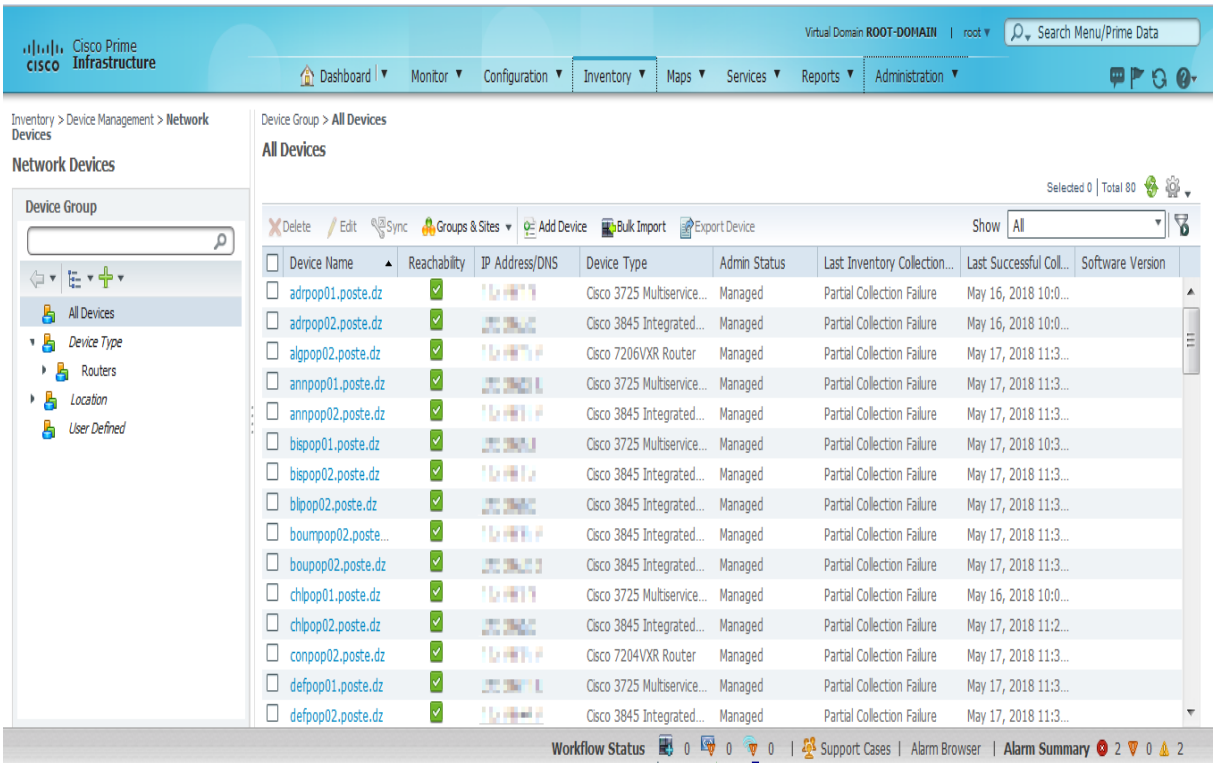
En cliquant sur **Buikl Import**, on importe le modèle de fichier qui est le suivant,



Par la suite on remplit les champs demandés dans le fichier, on enregistre, et enfin on parcourt ce fichier. La figure ci-dessous montre cette démarche.



On remarque d'après la notification que le fichier a été importé avec succès. Après l'actualisation de la page actuelle on obtient cela.

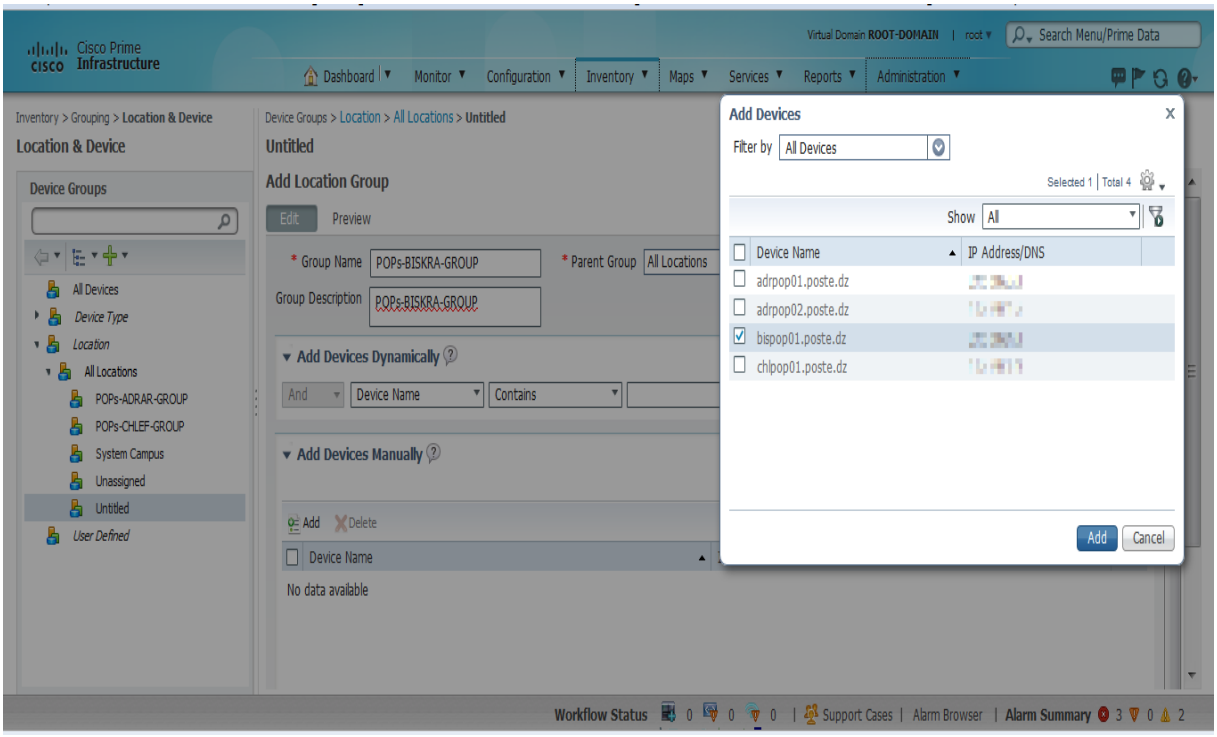


IV.3.3 Ajout d'un groupe :

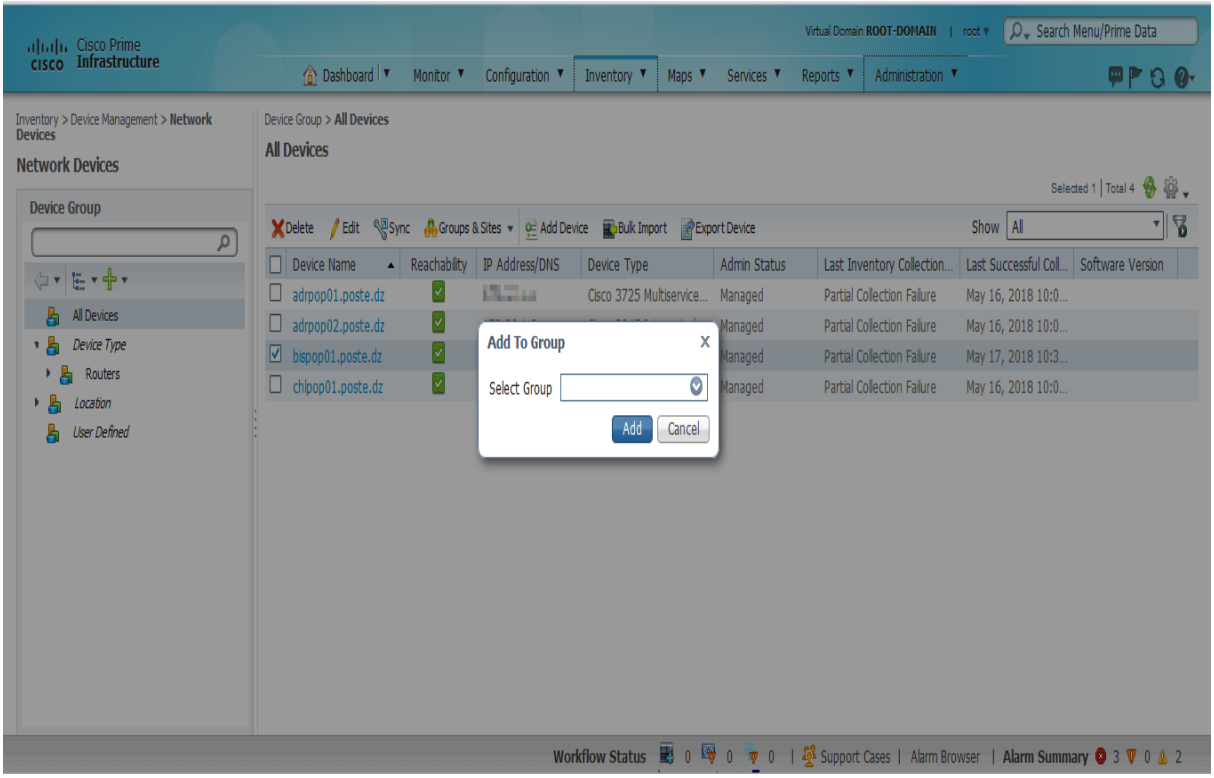
Pour que le travail soit plus organisé, on va vers l'ajout de groupes qui enveloppent les périphériques de chaque wilaya.

Pour cela on se dirige vers l'onglet **Inventory > Grouping > Location Devices.**

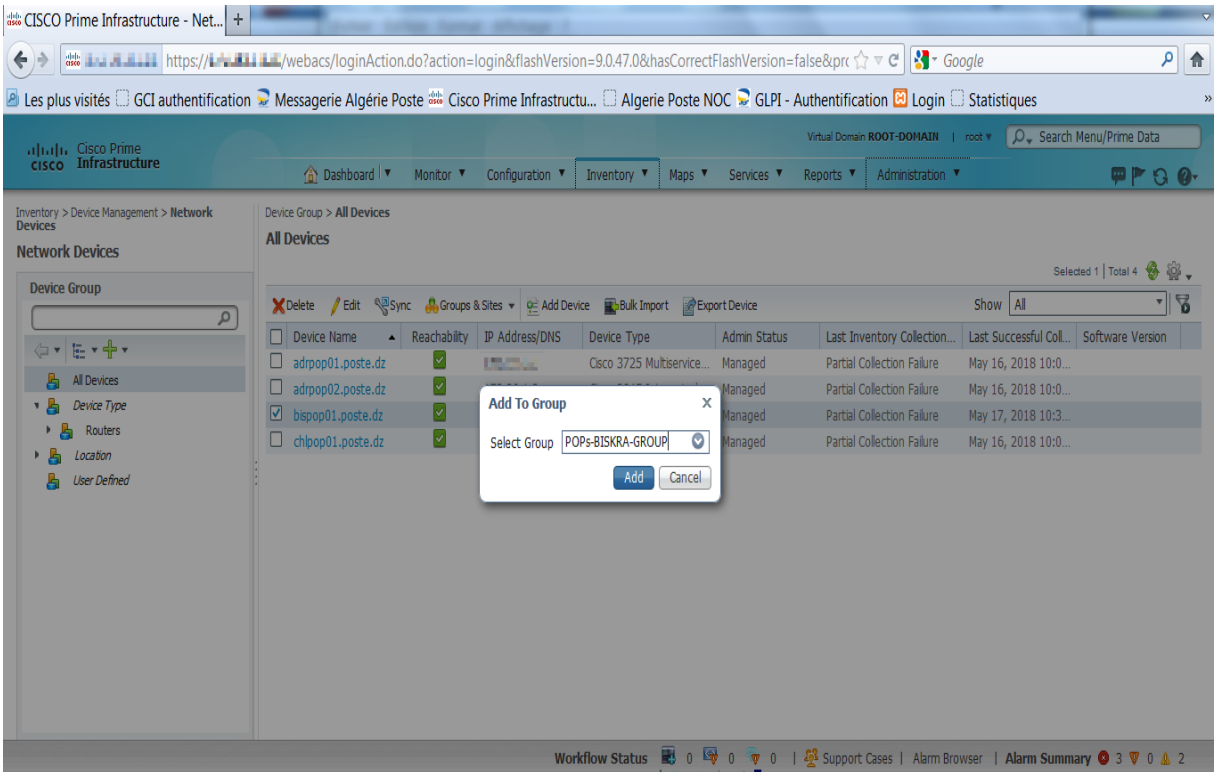
L'image ci-dessous montre l'ajout du groupe de PoPs de Biskra.



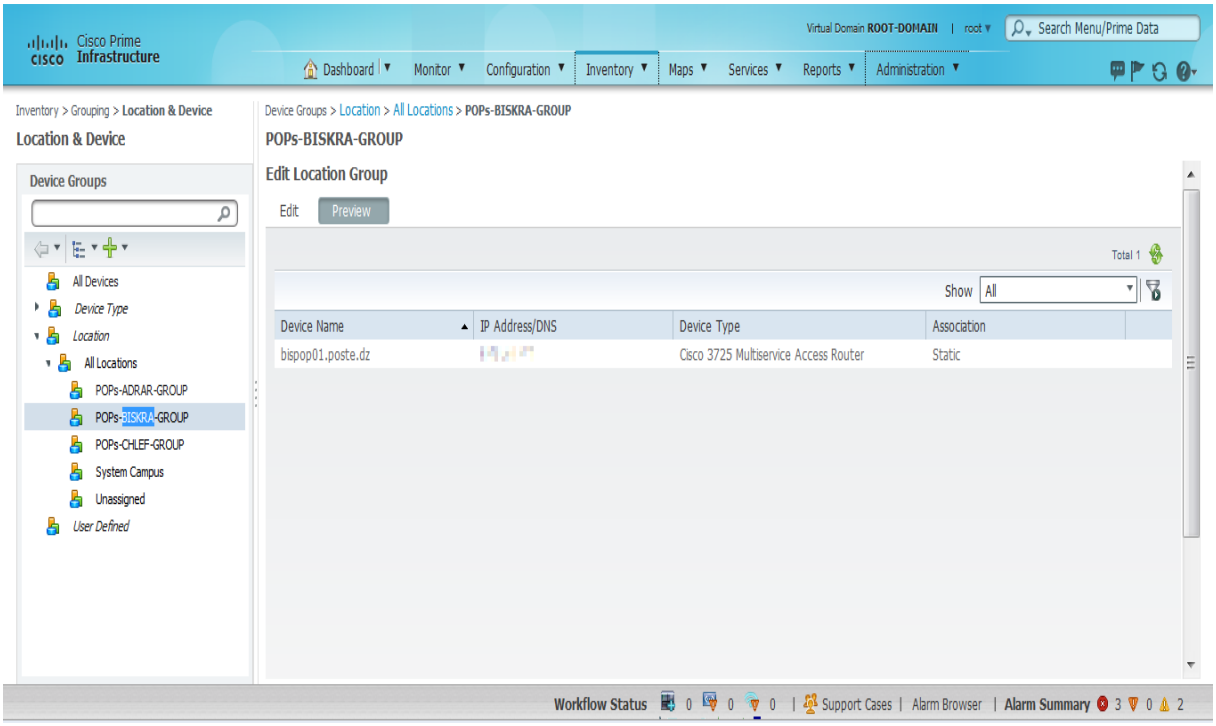
Dans ce qui suit, la figure démontre comment on a introduit les périphériques dans le groupe de Biskra.



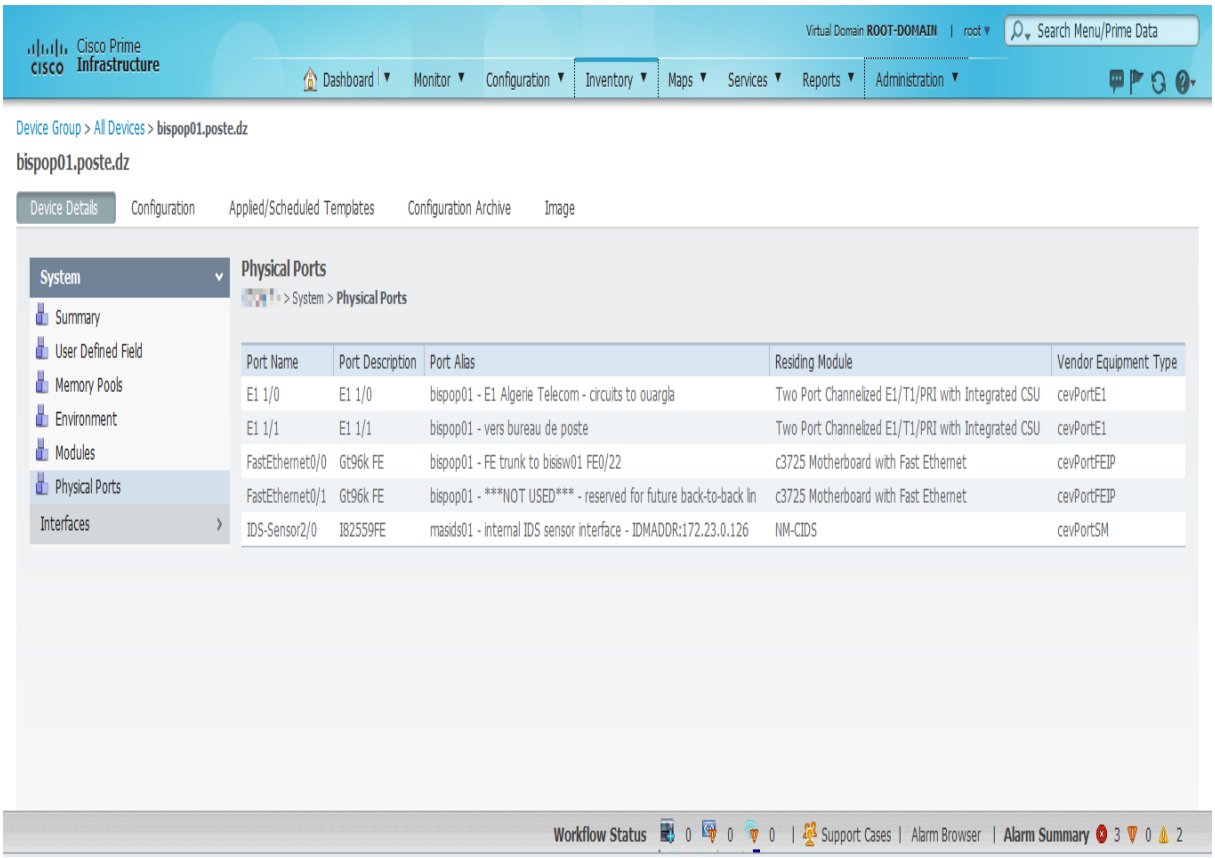
On a rempli le champs en déterminant le groupe adéquat.

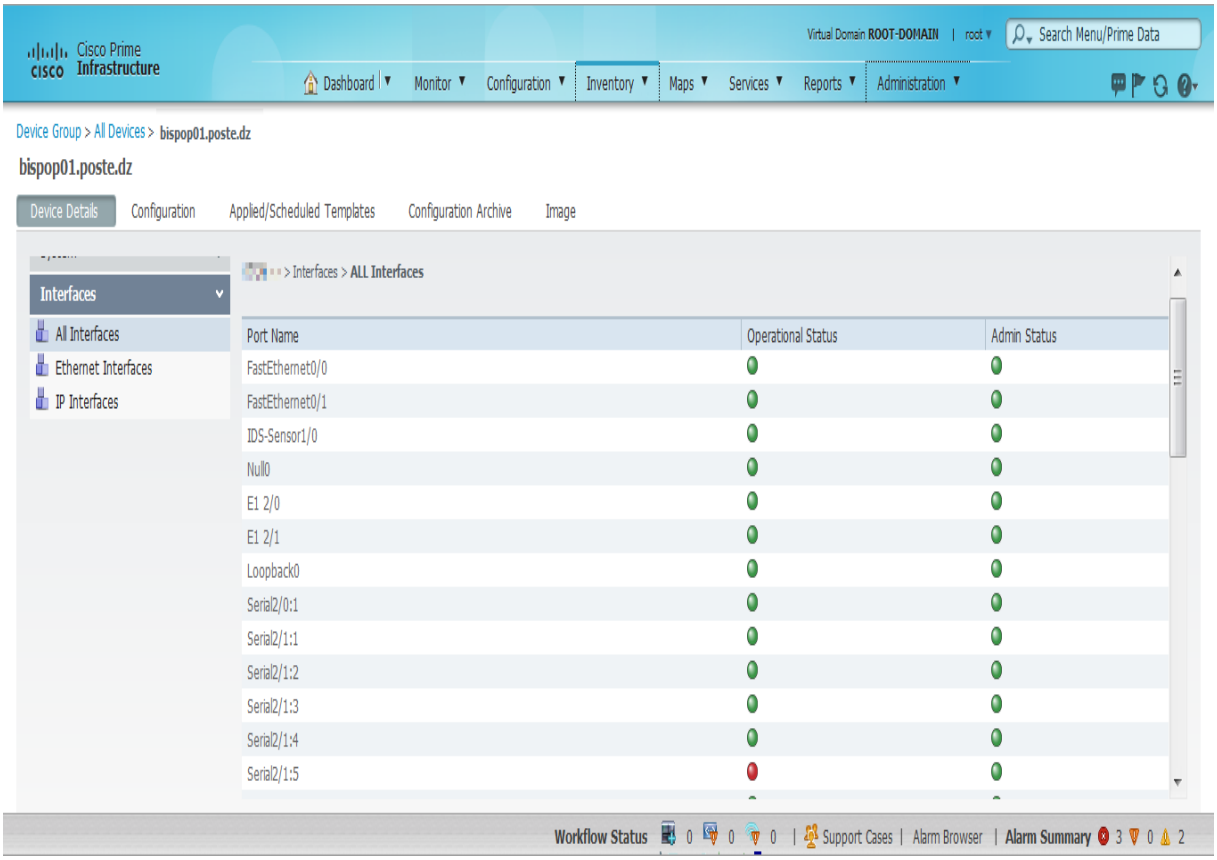


Ici l'ajout des PoPs dans le groupe a été approuvé.

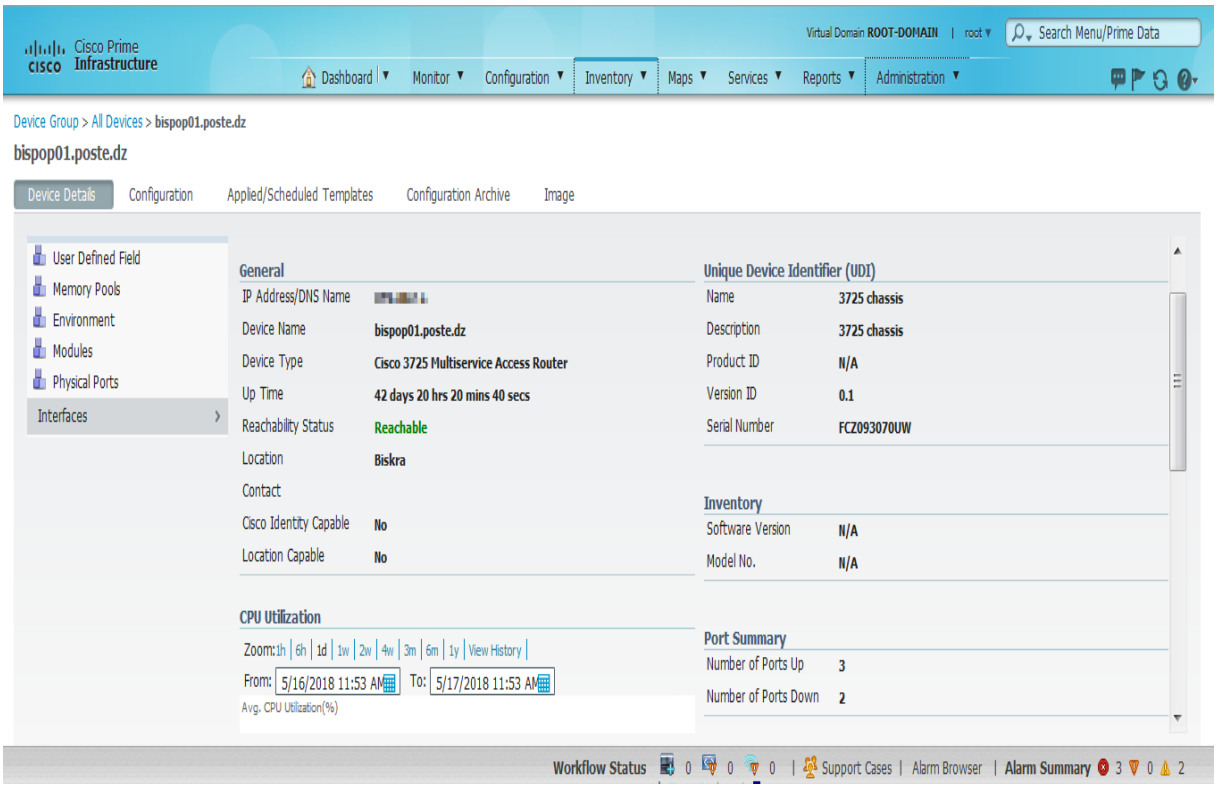


Détails concernant les ports physiques du PoP 01 de Biskra ainsi que ses interfaces.





Le récapitulatif des informations concernant le PoP 01 de Biskra.

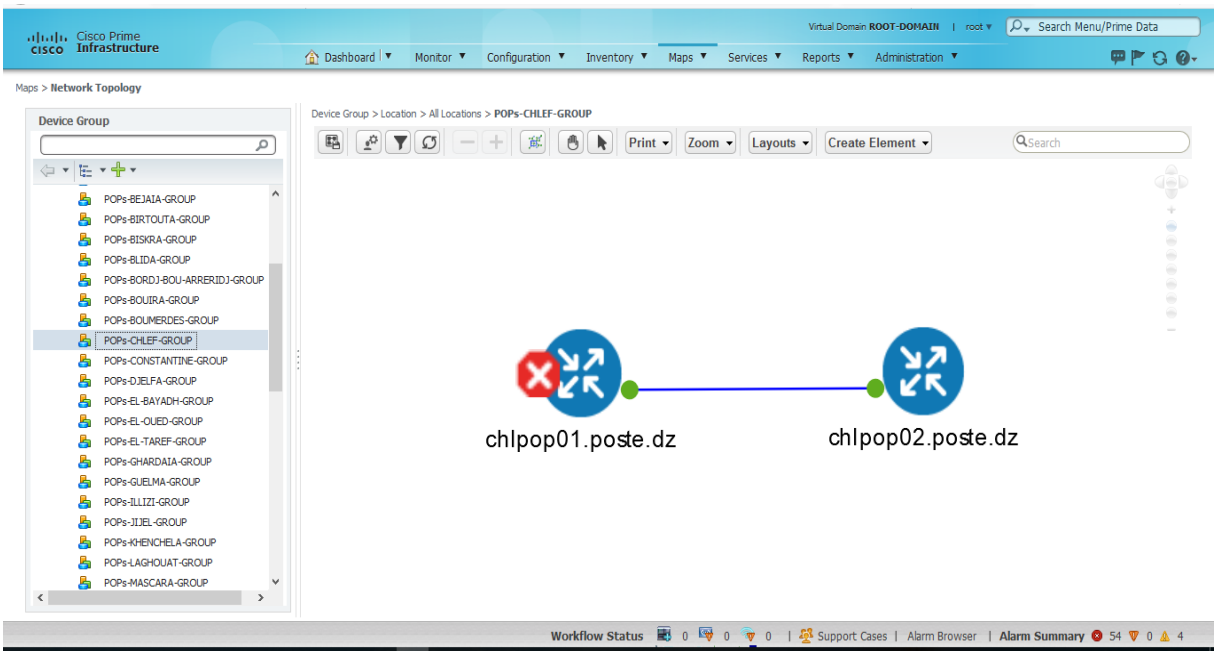


IV.3.4 Le Mapping :

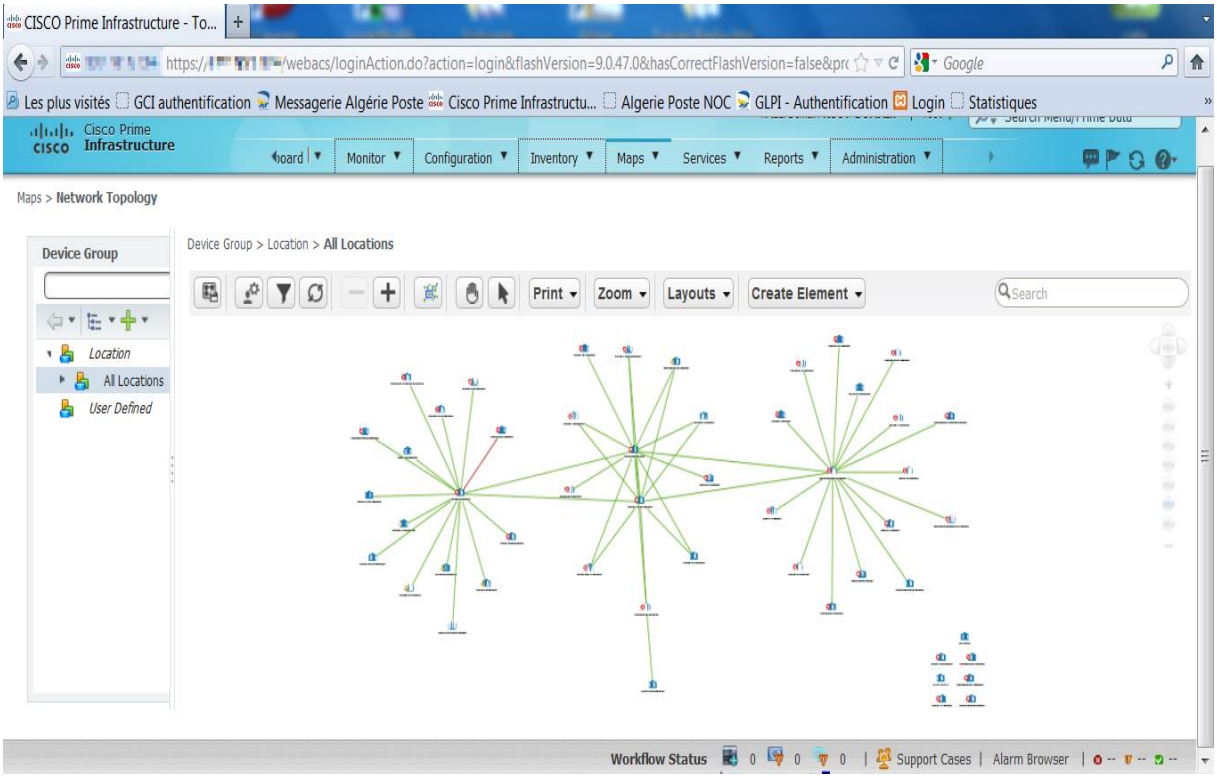
La Map est une fonctionnalité qui sert à schématiser les différents liens du réseau. Elle se trouve dans l'onglet **Maps > Network Topology.**

Le point vert de chaque extrémité montre que les périphériques sont en marche (Up). En cas de problème dans l'une des extrémités le point vert se transforme en rouge.

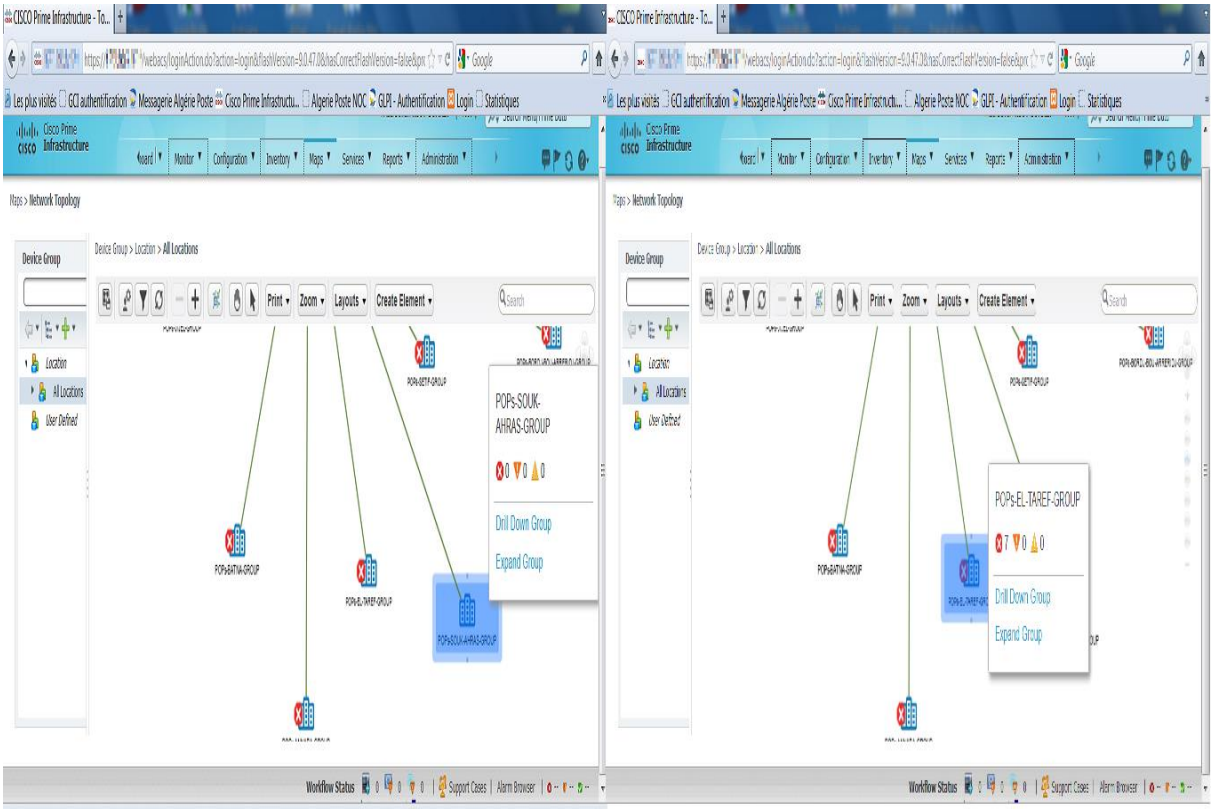
La figure ci-dessous montre le lien entre les deux PoPs se situant dans la wilaya de Chlef.



La Map ci-dessous englobe l'ensemble des points de présence de l'entreprise.



Détails de l'état du PoP de Souk Ahras et El Taref via la Map.



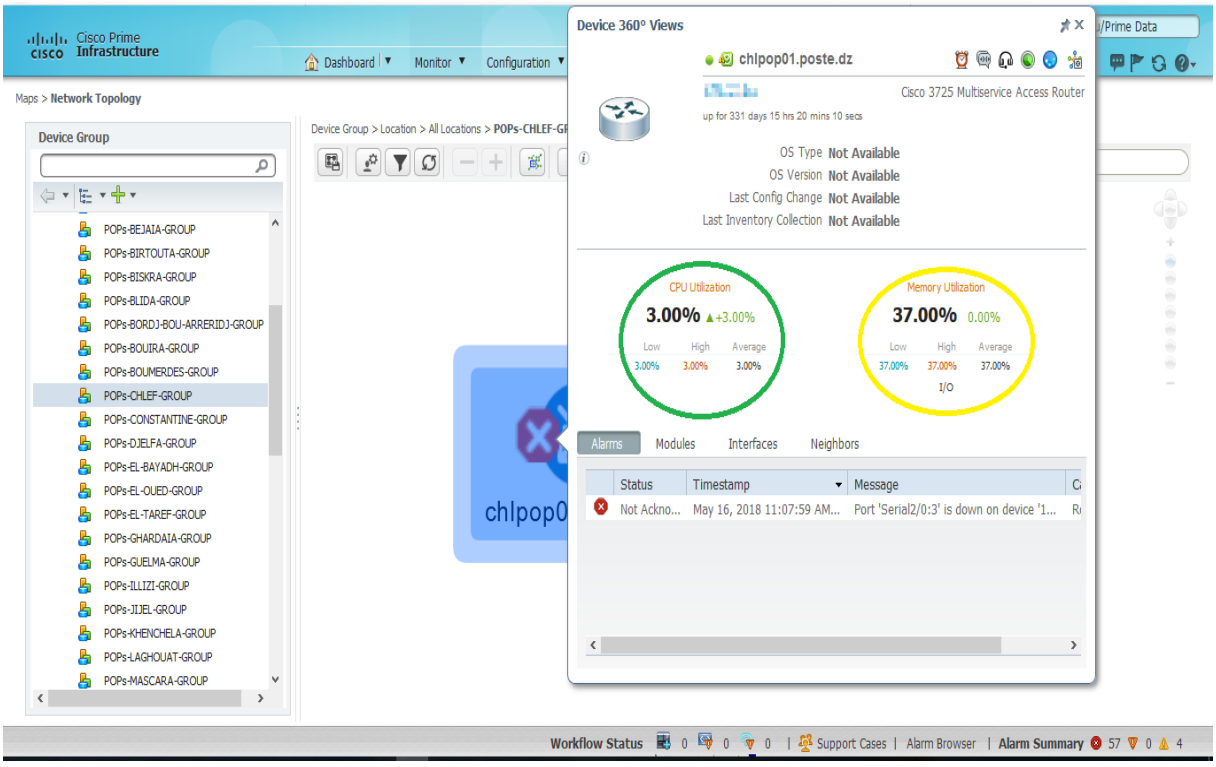
IV.3.5 Device 360° Views :

Cette fonctionnalité permet de donner à l'utilisateur toutes les informations correspondantes à un ou un groupe de périphériques englobées dans une même page

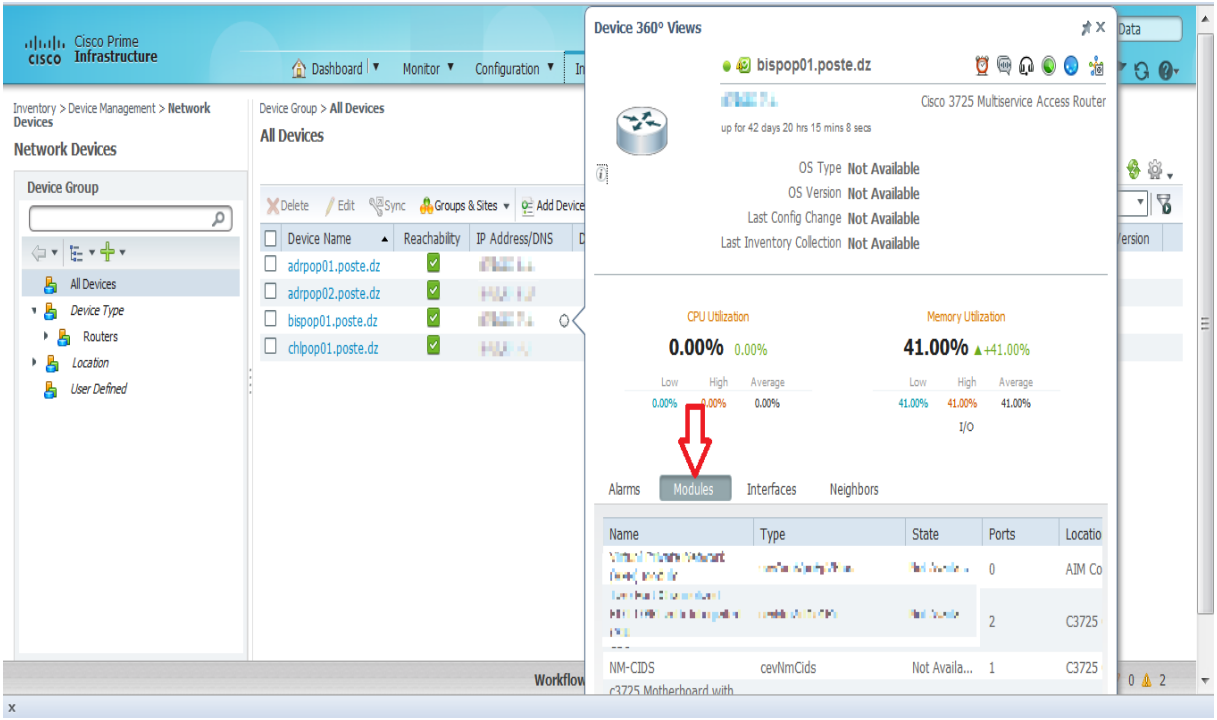
L'image ci-dessous montre deux cercles ; vert et jaune. Le vert correspond au pourcentage d'utilisation du CPU, le jaune correspond à son tour au pourcentage de mémoire utilisée avec des détails (law, high, average).

On remarque en bas de la page des onglets comprenant des fonctionnalités telles que : Alarms, Modules, Interfaces, Neighbors.

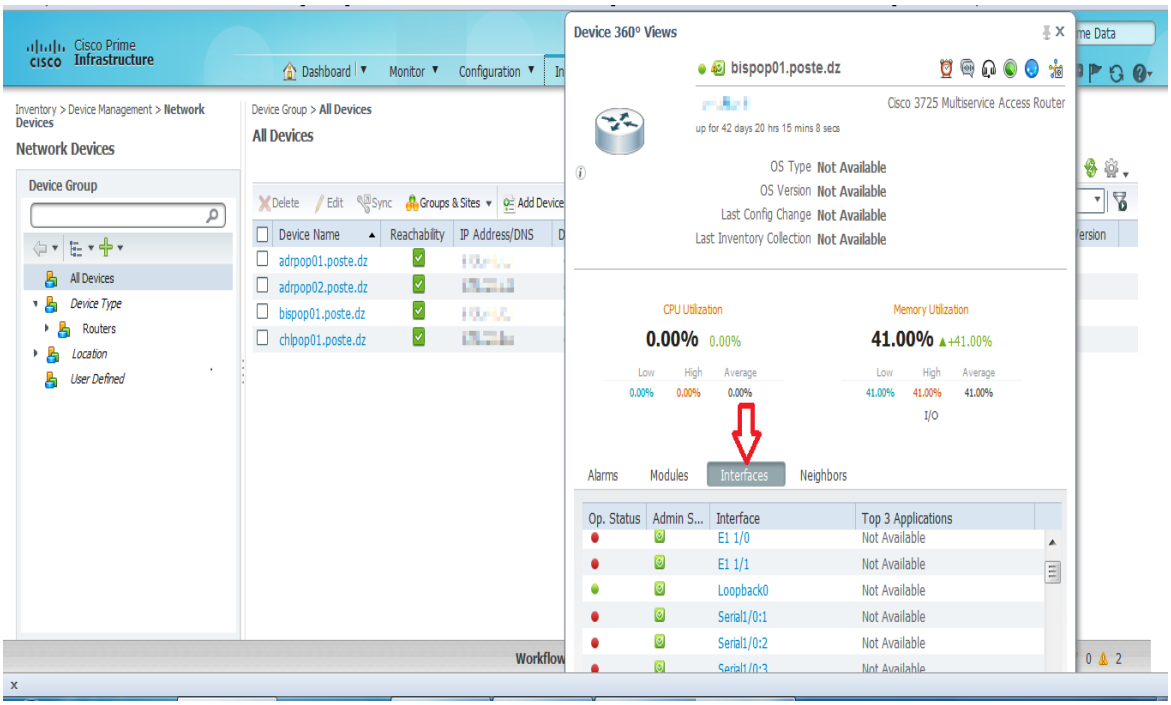
- ✓ La fonctionnalité alarms : Répertorie les alarmes sur la plateforme, y compris l'état de l'alarme, l'horodatage et la catégorie.



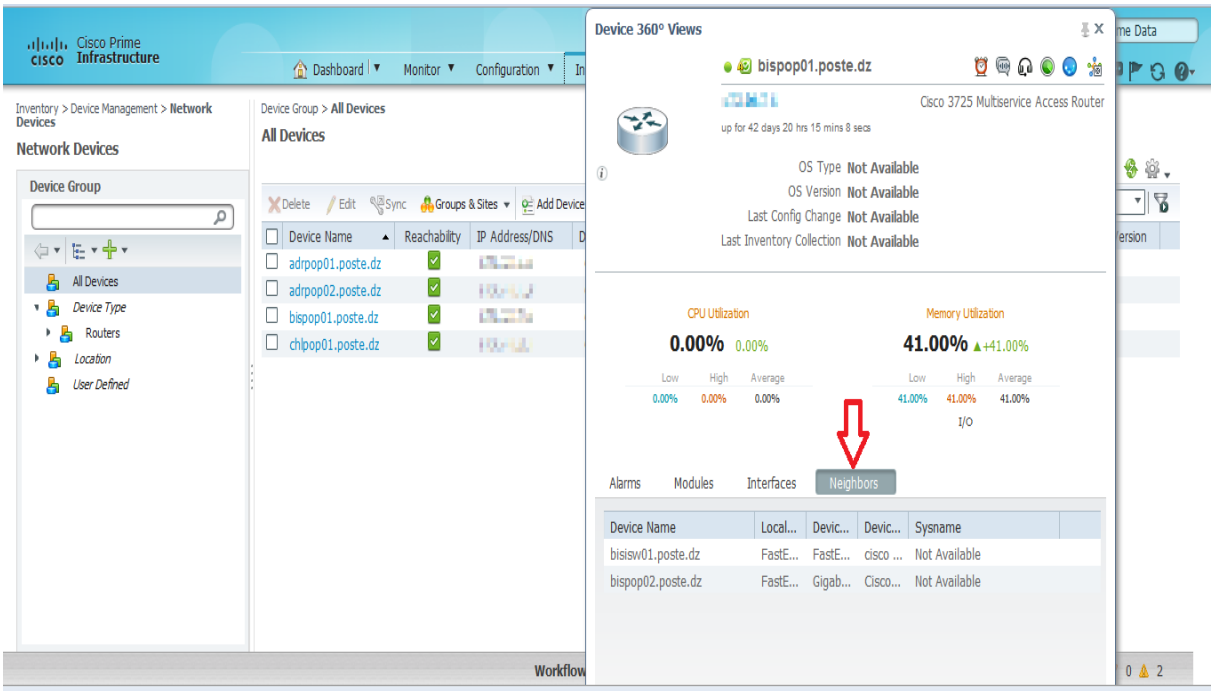
- ✓ La fonctionnalité module : Liste les modules de périphériques et leurs noms, type, état et ports.



✓ La fonctionnalité interfaces : Répertorie les interfaces de périphérique et les trois premières applications pour chaque interface.



✓ La fonctionnalité neighbors : Répertorie les voisins du périphérique, y compris leur index, leur port, leur état de duplex et leur nom de système.



IV.3.6 Configuration de notifications :

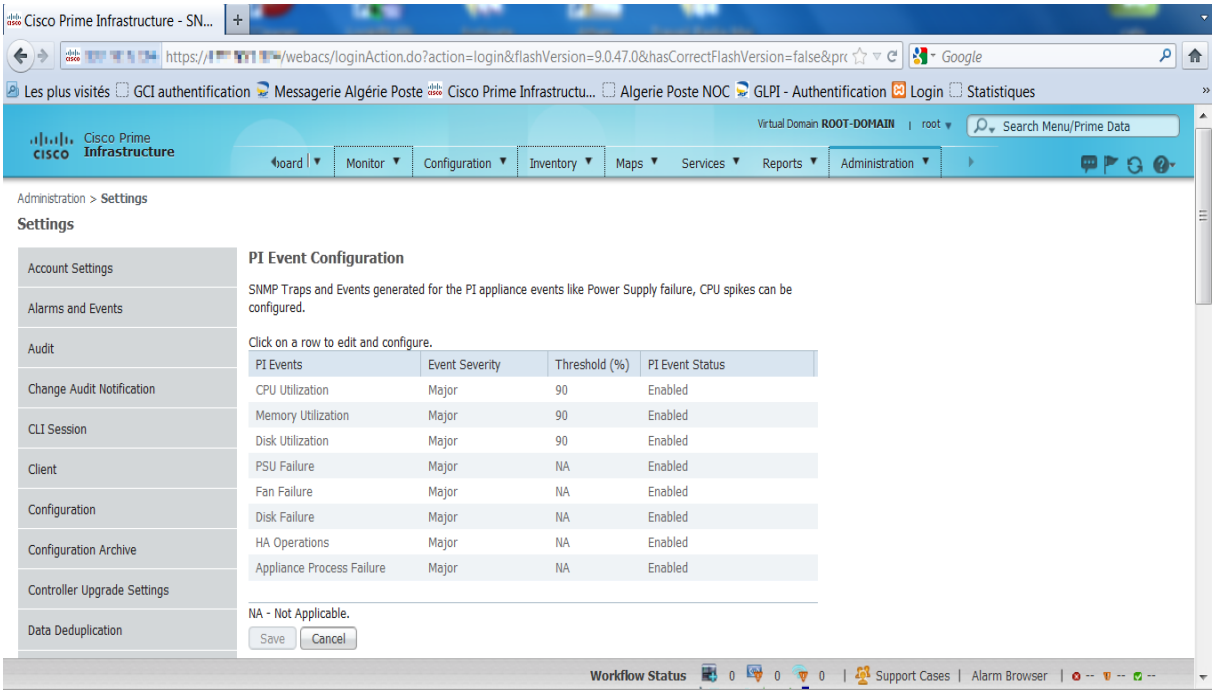
Pour que Prime Infrastructure envoie des notifications d'interruption SNMP au northbound, on doit configurer les bons paramètres sur les pages de notifications d'événements et celle de destinataires de notification. Une fois configurés, les interruptions seront générées en fonction des valeurs associées au seuil et à la gravité d'événements SNMP suivants:

- Échec du processus de l'appliance ;
- Opérations HA ;
- Utilisation du processeur, du disque et de la mémoire ;
- Défaillance du disque, du ventilateur et de l'alimentation ;

On peut modifier le seuil et la gravité associés à chaque événement et activer ou désactiver la génération d'interruptions pour l'événement associé.

Étape 1 : Se connecter à Prime Infrastructure à l'aide d'un ID utilisateur avec des privilèges d'administrateur.

Étape 2 : On sélectionne **Administration > Settings > PI Event Notification.**



Étape 3 : Pour chaque événement SNMP qu'on souhaite configurer:

a. On clique sur la ligne de cet événement.

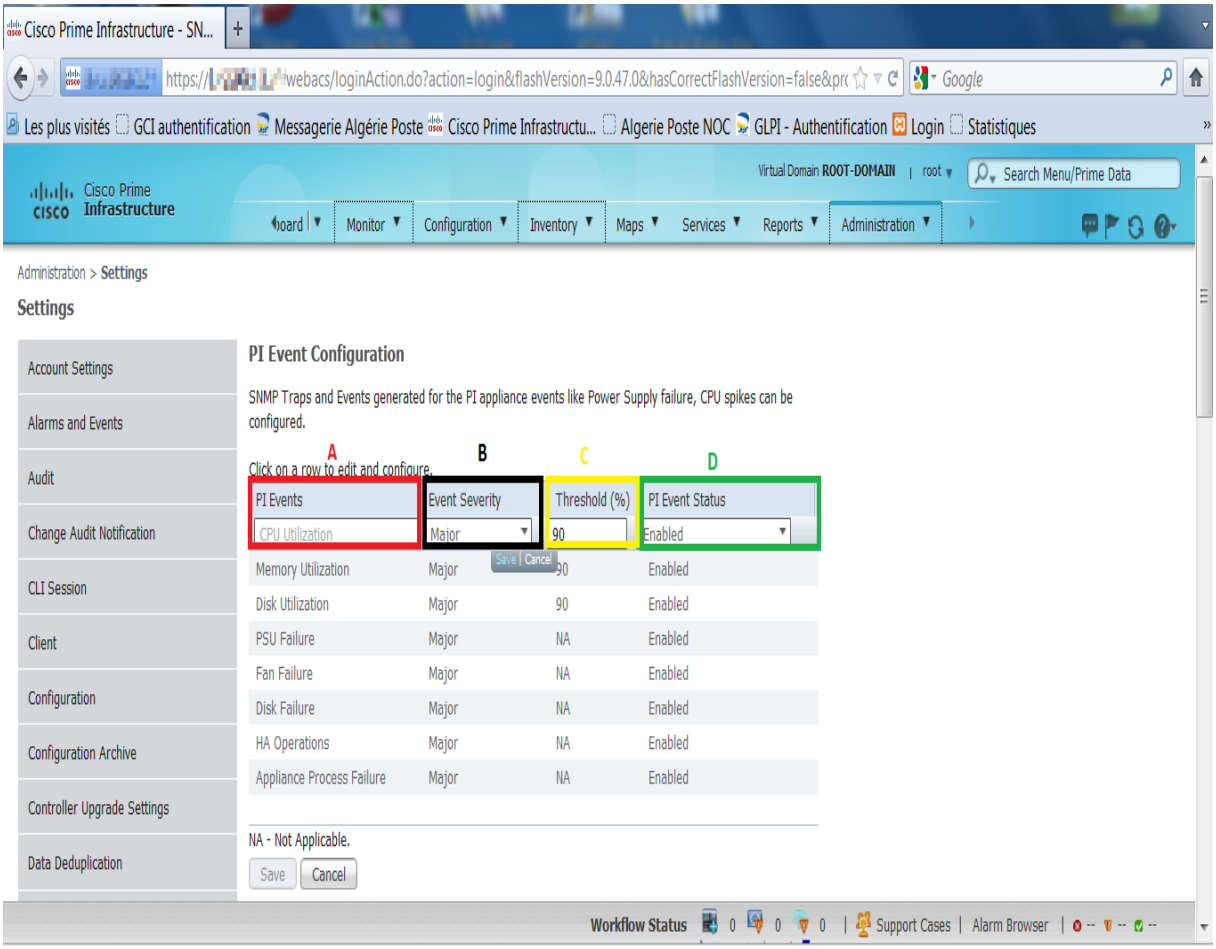
b. On définit le niveau de gravité de l'événement sur Critique, Majeur ou Mineur, selon les besoins.

c. Pour les interruptions d'utilisation du processeur, du disque et de la mémoire: on définit le pourcentage de seuil (compris entre 1 et 99).

Ces événements enverront les interruptions SNMP associées lorsque l'utilisation dépasse la limite de seuil.

On ne peut pas définir de seuils pour les événements pour lesquels le paramètre de seuil est défini sur NA. Ces événements envoient des interruptions chaque fois que la défaillance associée est détectée.

d. Nous définissons l'état de l'événement SNMP sur Activé ou Désactivé. Si on le définit sur Enabled, la trap correspondante sera générée pour cet événement.



Étape 4 : Cliquer sur **Save** pour sauvegarder les changements.

IV.3.7 Configuration des récepteurs de notification :

Une fois que nous avons activé les notifications d'interruption et personnalisé leurs sévérités et leurs seuils, on passe à la configuration d'un ou plusieurs récepteurs de notification pour recevoir les interruptions.

Lorsque nous ajoutons un récepteur de notification, n'oublions pas de sélectionner la case à cocher Système comme l'un des critères et définir **Severity** sur la gravité la plus élevée définie sous le niveau de sévérité configuré pour chaque interruption sur la page de notifications d'événements.

Étape 1 : On se connecte à Prime Infrastructure avec un ID utilisateur disposant des privilèges d'administrateur.

Étape 2: On sélectionne **Administration > System Settings > Notification Receivers.**

Étape 3 : Dans la boîte de dialogue **Select a command**, on sélectionne **Add Notification Receiver**, puis on clique sur OK.

Étape 4 : On Rempli les champs suivants comme le montre la figure :

a. **Adresse IP :** l'adresse IPv4 ou IPv6 du serveur sur lequel le récepteur sera exécuté.

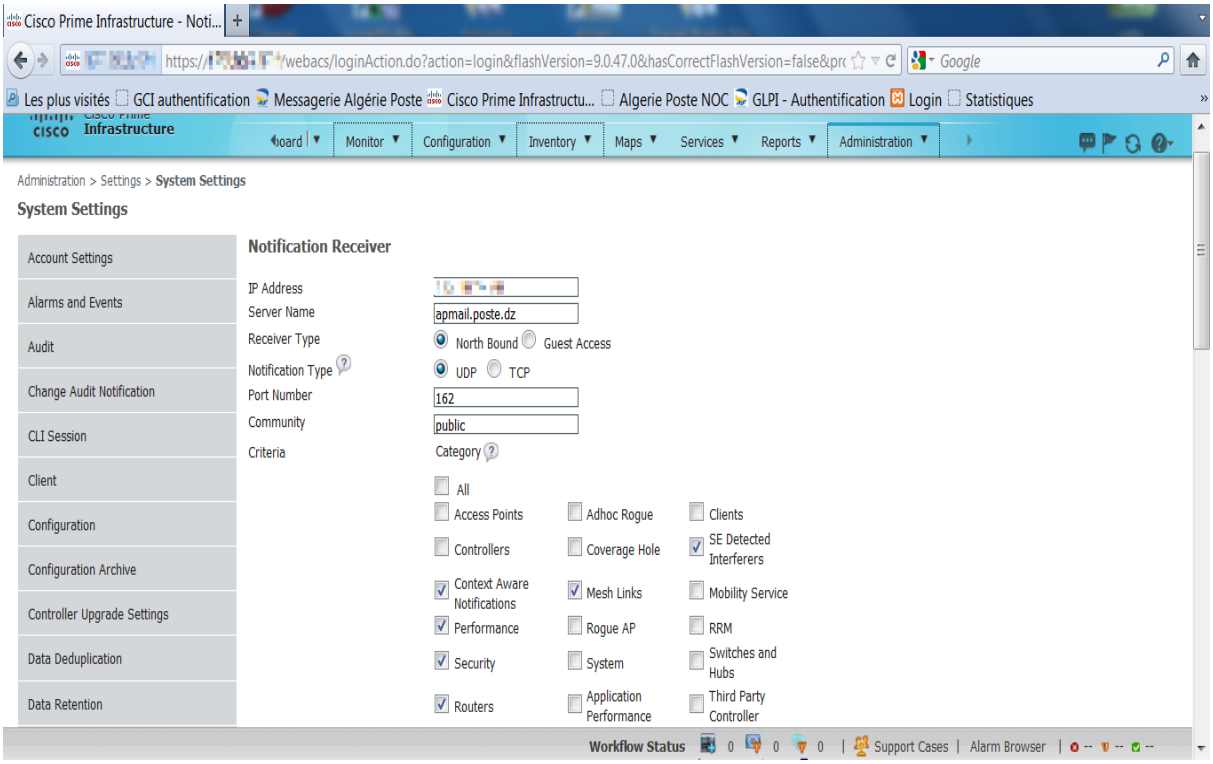
b. **Nom du serveur :** le nom d'hôte du serveur sur lequel le récepteur sera exécuté.

c. **Type de récepteur :** on sélectionne Northbound

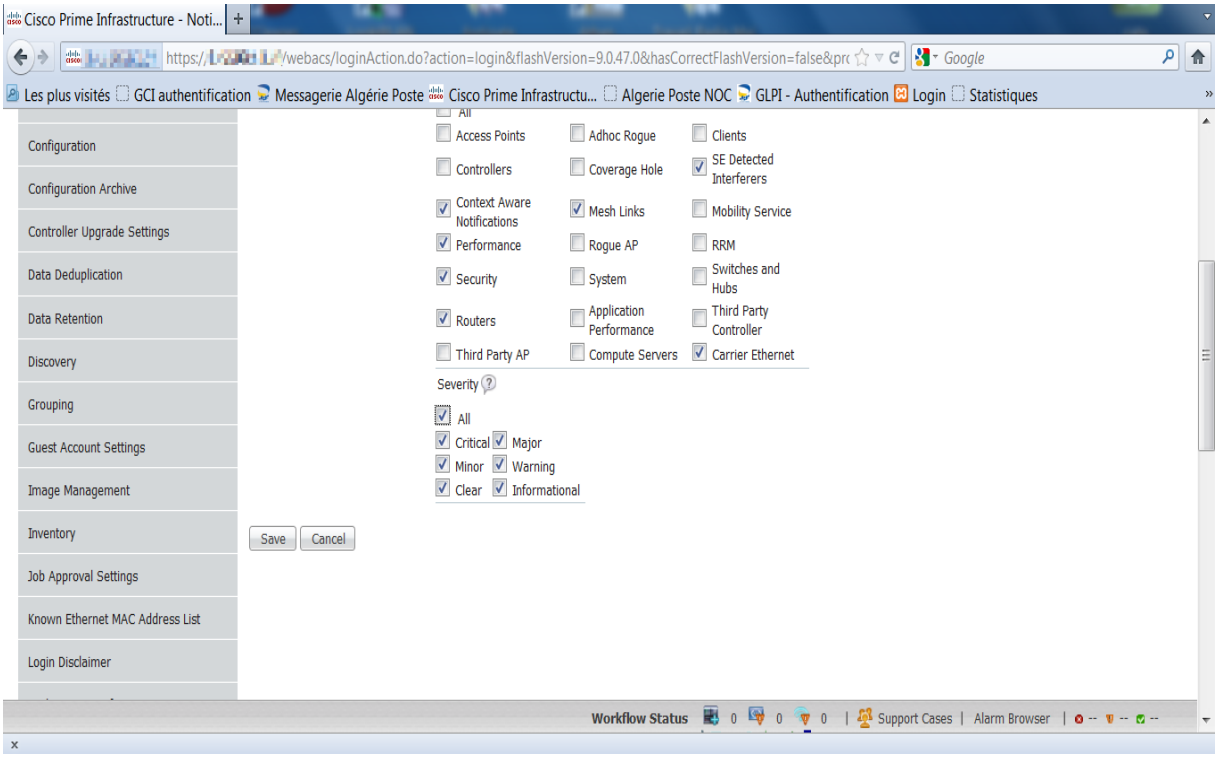
d. **Type de notification :** on sélectionne UDP.

e. **Numéro de port :** 162

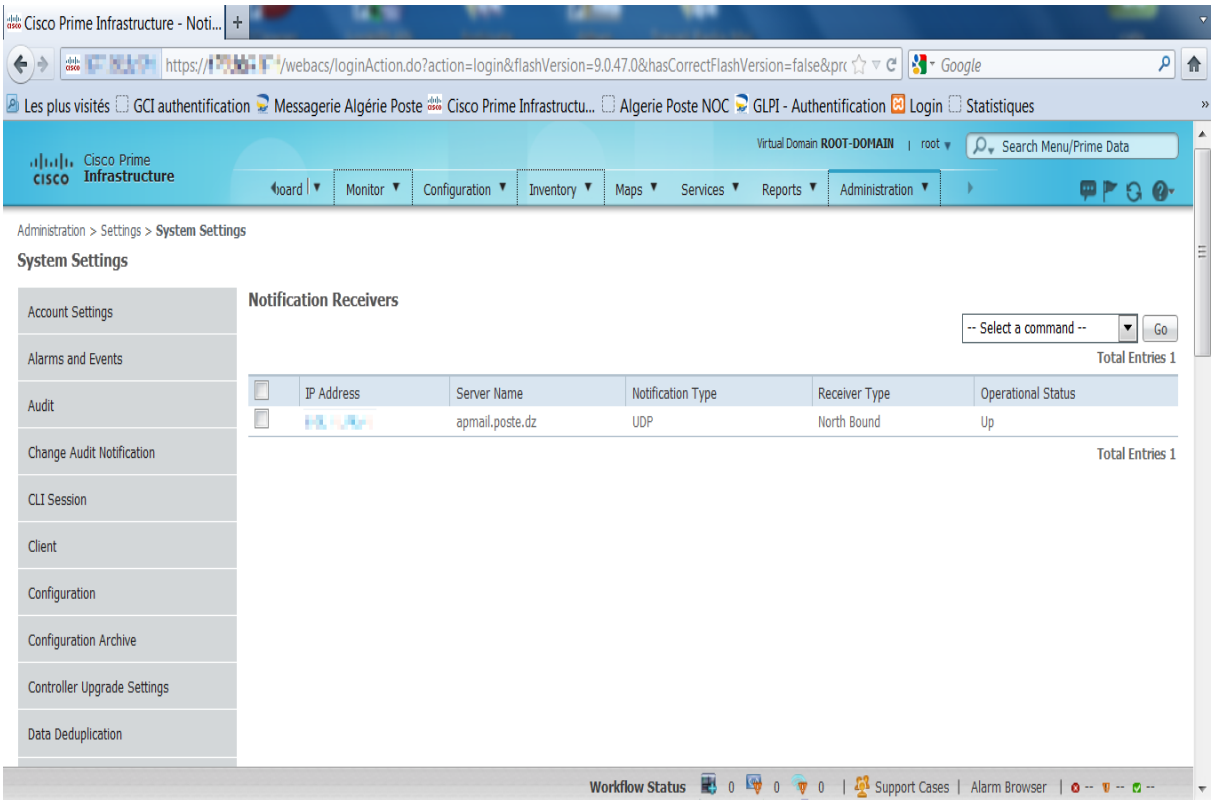
f. **Critères :** On coche la catégorie de critères sur lesquels on veut être notifiés ainsi que les types de gravité.



Étape 5 : Lorsqu'on termine, on clique sur **Save**.



La figure ci-dessous montre que l'ajout du récepteur de notifications a été effectué.



IV.3.8 Configuration des notifications par courrier électronique pour les interruptions SNMP :

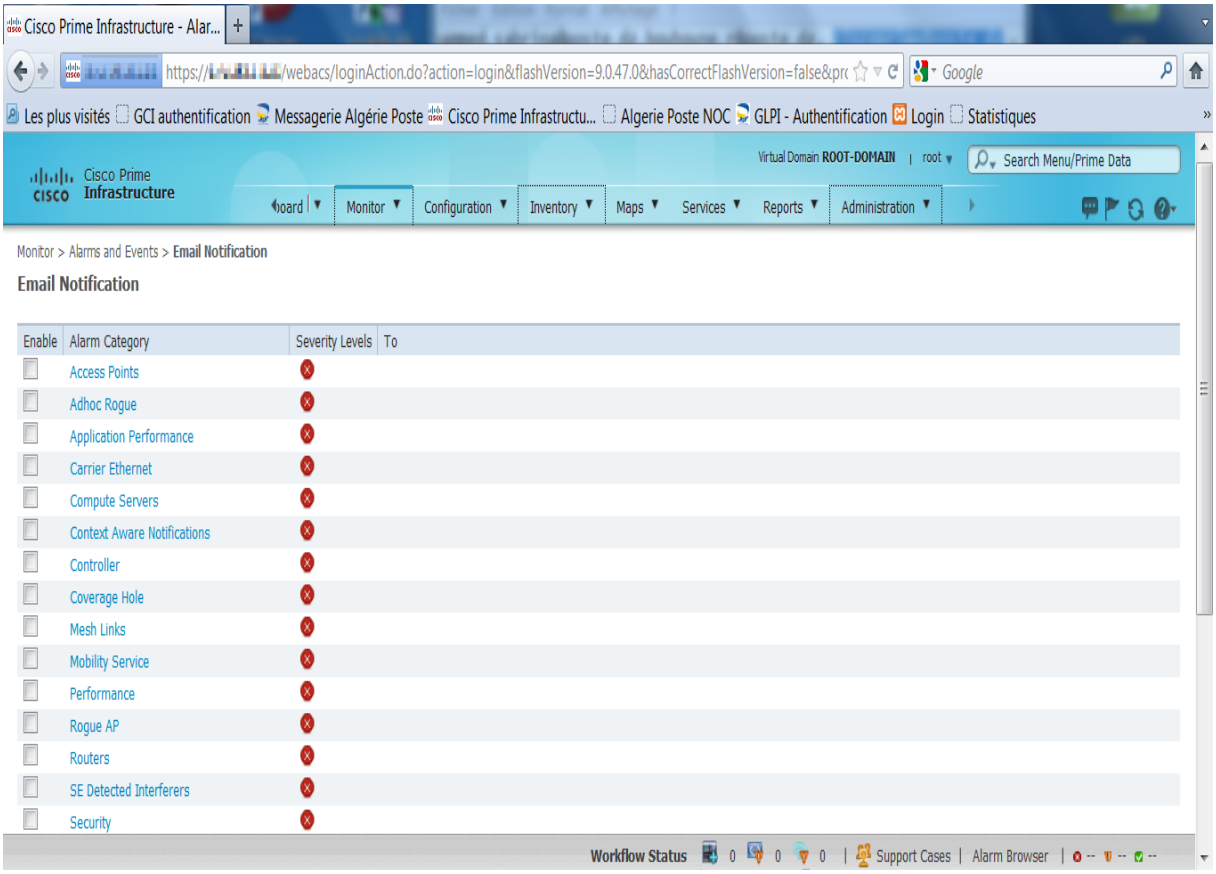
On peut configurer Prime Infrastructure pour envoyer une notification par courrier électronique pour les alarmes et les événements générés dans les réponse aux interruptions SNMP. Toutes ces alarmes et événements sont considérés comme faisant partie de la catégorie d'événement Système.

On peut également personnaliser le niveau de sévérité pour lequel ces notifications seront envoyées. Notons que, pour que ces notifications par e-mail soient envoyées, un administrateur de Prime Infrastructure doit configurer au moins un serveur de messagerie SMTP principal.

Étape 1 : Se connecter à Prime Infrastructure.

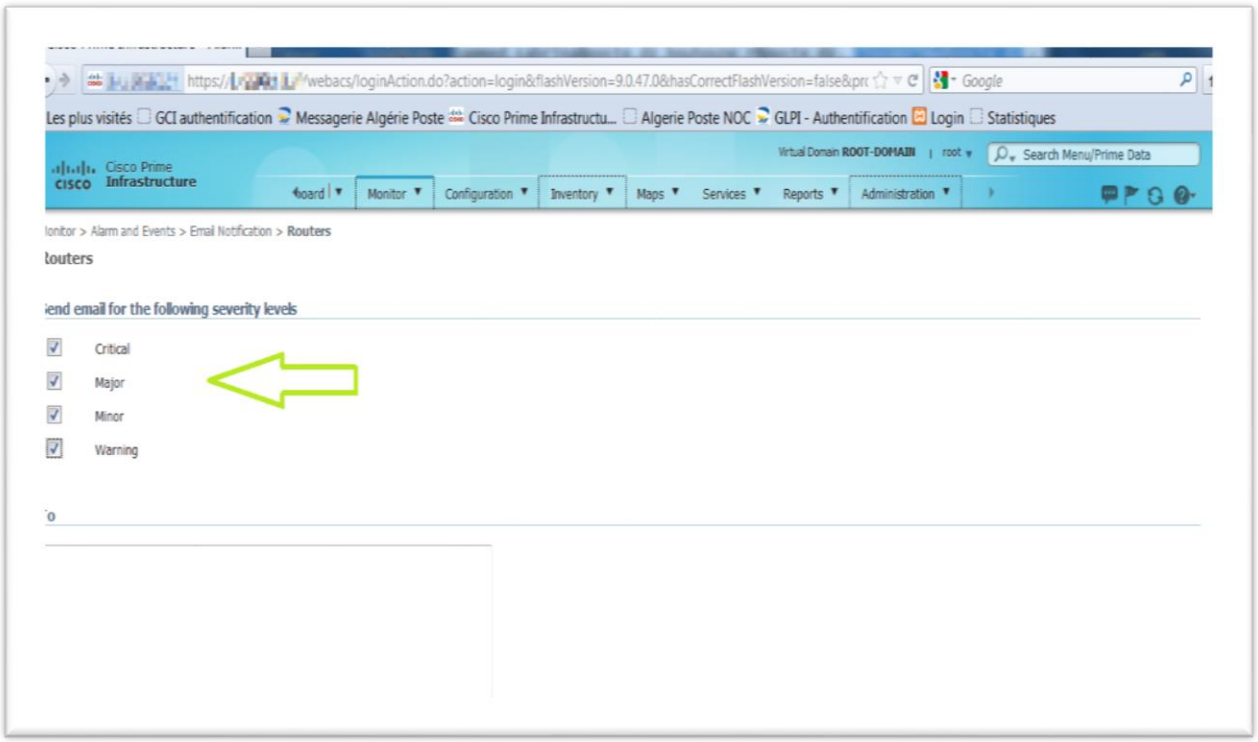
Étape 2 : On sélectionne **Monitor > Alarms and Events.**

Étape 3 : On clique sur **Email Notification**. L'infrastructure principale affiche la première page de paramètres de notification par courrier électronique.



Étape 4 : Dans la colonne **Alarm Category**, on clique sur le nom de la catégorie **System**. Prime Infrastructure affiche un deuxième page Paramètres de notification par e-mail.

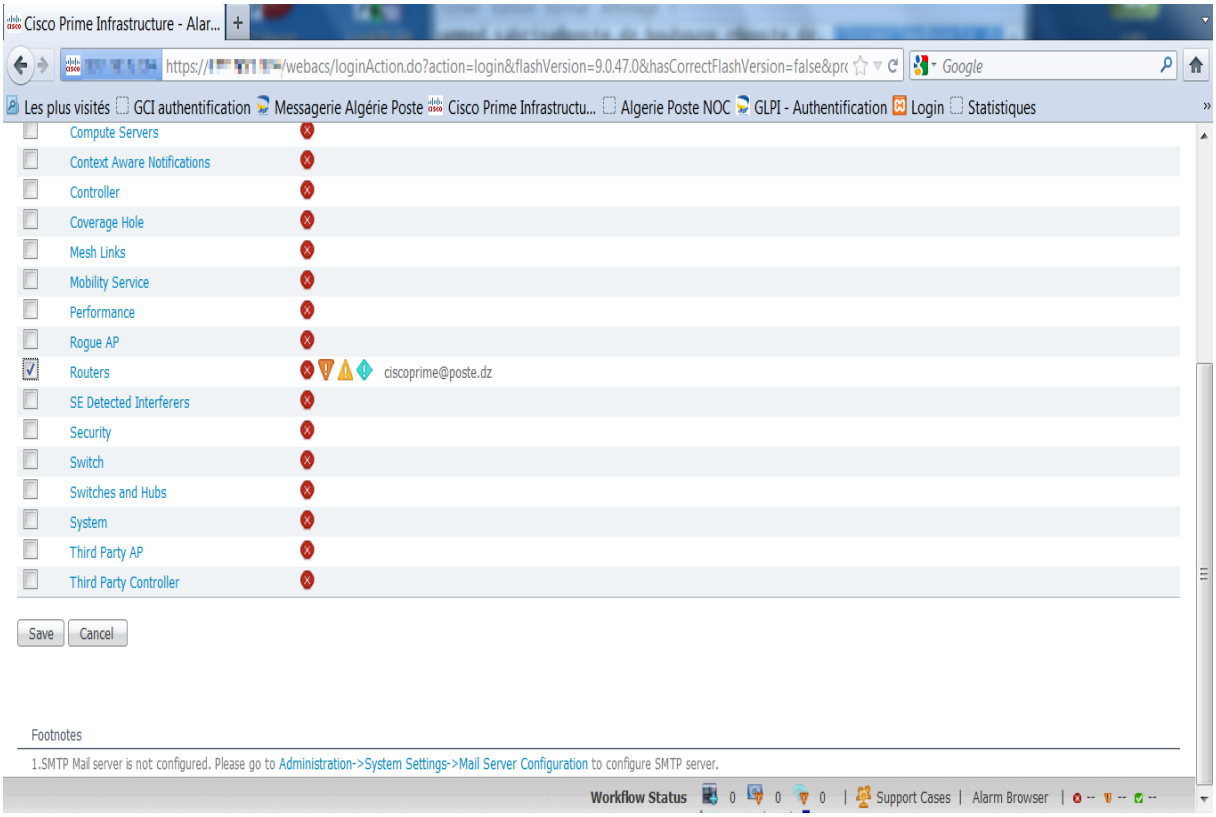
Étape 5 : Dans **Send email for the following severity levels**, on sélectionne tous les niveaux de sévérité qu'on souhaite pour que Prime Infrastructure envoie des notifications par e-mail.



Étape 6 : Dans **To**, on entre l'adresse électronique à laquelle on souhaite que Prime Infrastructure envoie des notifications par courrier électronique. Si on possède plusieurs adresses e-mail, on peut toutes les rajouter sous forme d'une liste séparée par des virgules.

Étape 7 : On clique sur **Save**. L'infrastructure principale affiche la première page des paramètres de notification par courrier électronique.

Étape 8 : Dans la colonne **Enable**, on s'assure que **System** est sélectionné, puis cliquez sur **Save**.



IV.3.8 Configuration des paramètres du serveur de messagerie :

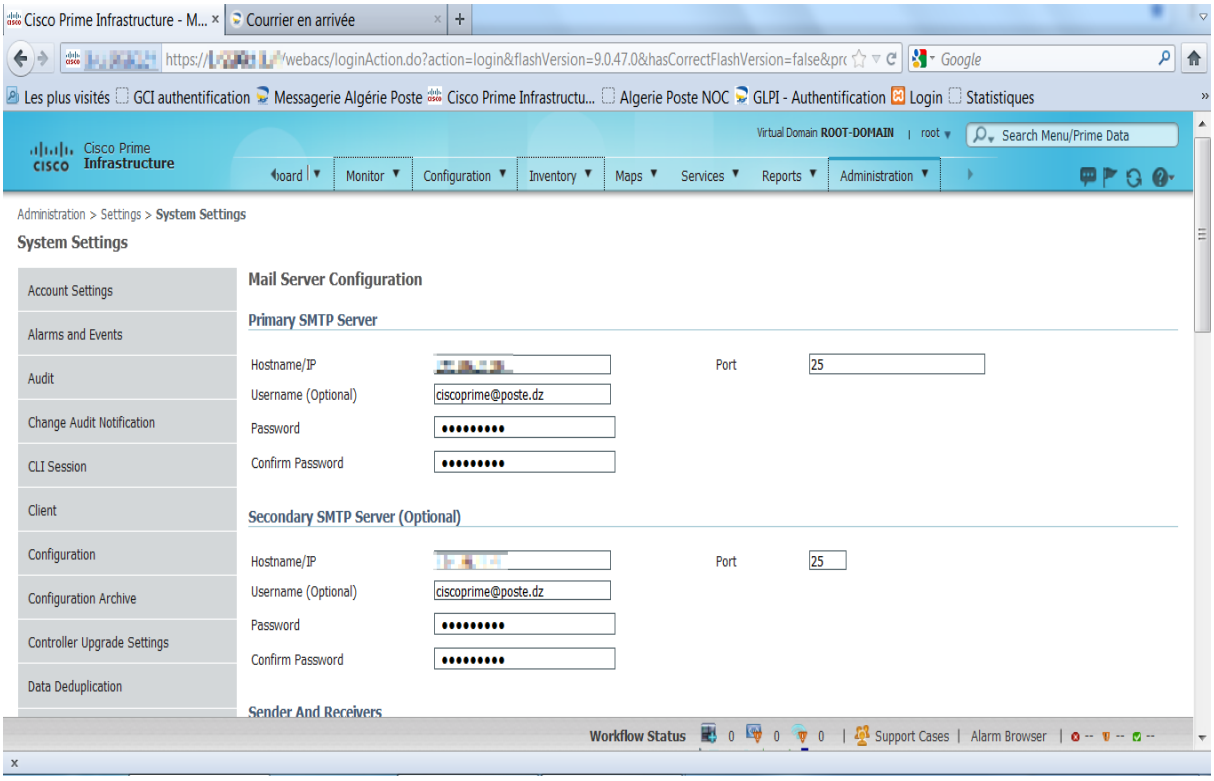
Pour permettre à Prime Infrastructure d'envoyer des notifications par courrier électronique, l'administrateur système doit configurer un serveur de messagerie SMTP principal (et, de préférence, un serveur de messagerie secondaire).

Étape 1 : On se connecte à Prime Infrastructure à l'aide d'un ID utilisateur avec des privilèges d'administrateur.

Étape 2 : On sélectionne **Administration > Settings > System Settings > Mail Server Configuration**.

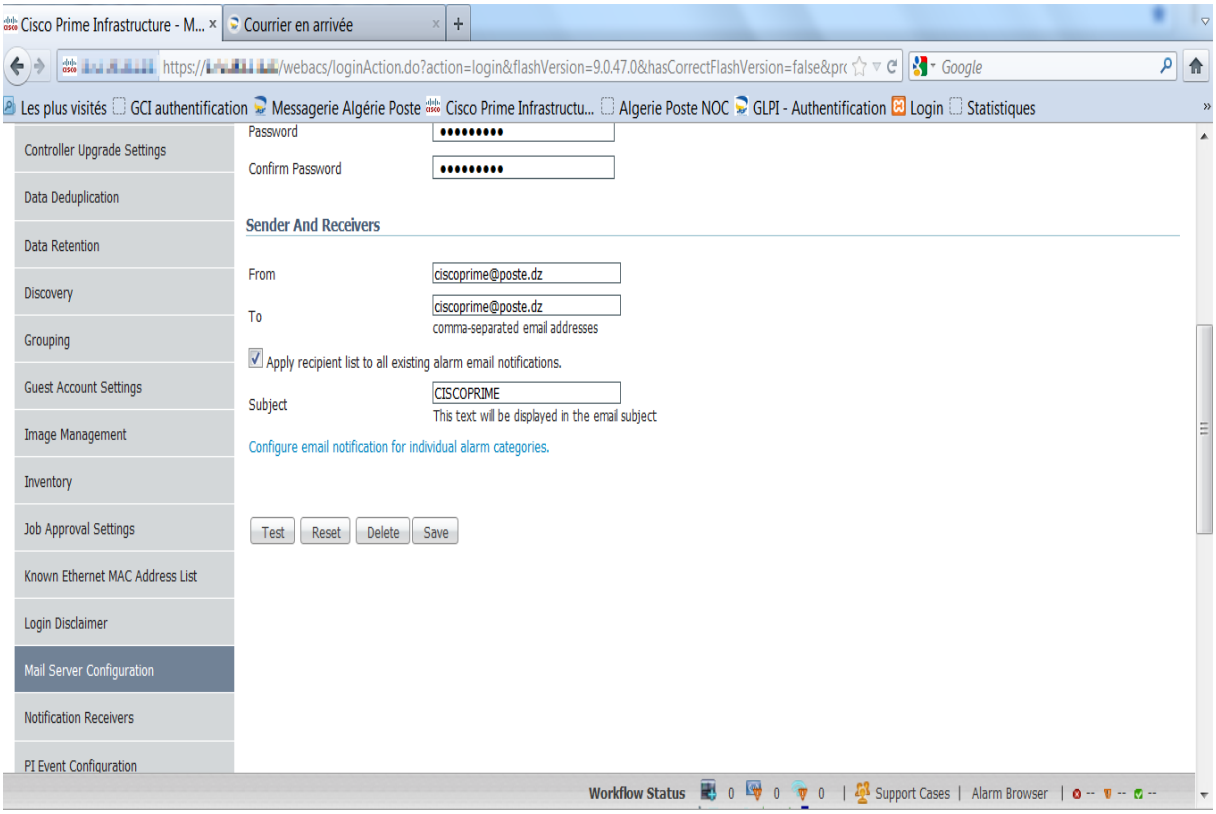
Étape 3 : Sous le serveur SMTP principal, on complète **Hostname/IP**, **User Name**, **Password** et on confirme **le password** correspondant au serveur de messagerie que Prime Infrastructure doit utiliser.

Étape 4 : (Optionnel) On remplit les mêmes champs sous **Secondary SMTP Server,** si on souhaite avoir un serveur SMTP secondaire.



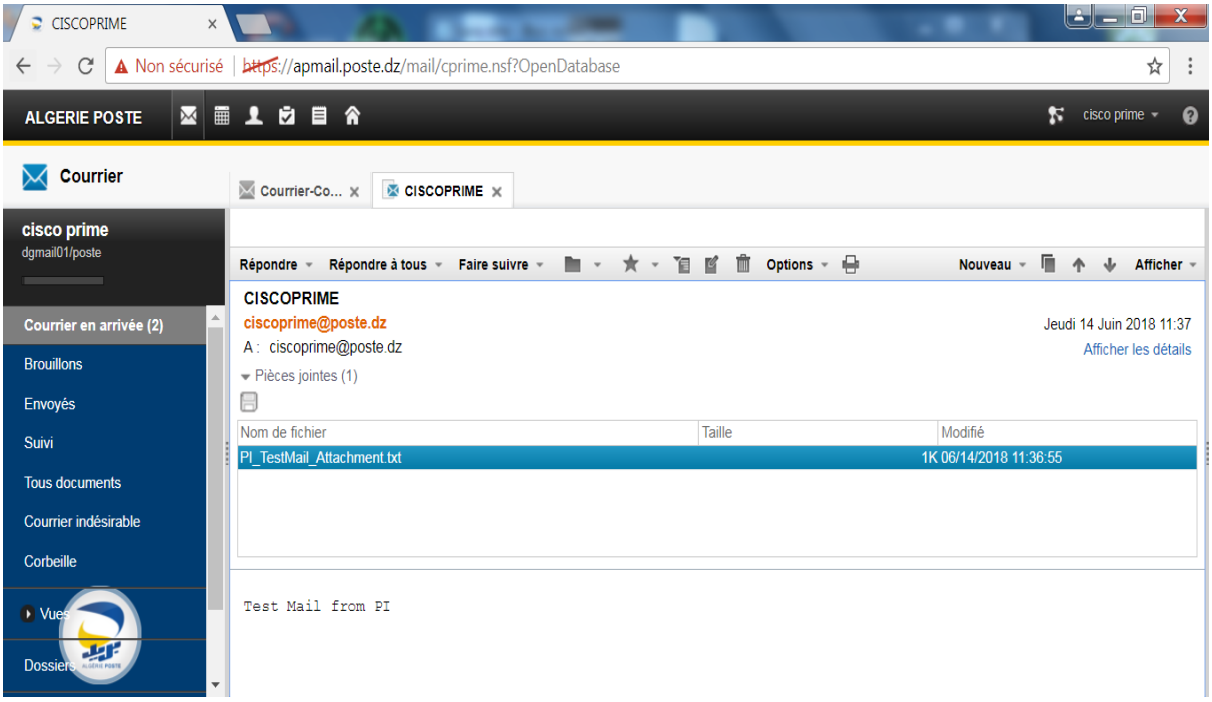
Étape 5 : Dans **Sender and Receivers**, on saisit l'adresse électronique légitime pour le serveur Prime Infrastructure.

Étape 6 : Lorsqu'on termine, on clique sur **Save**.

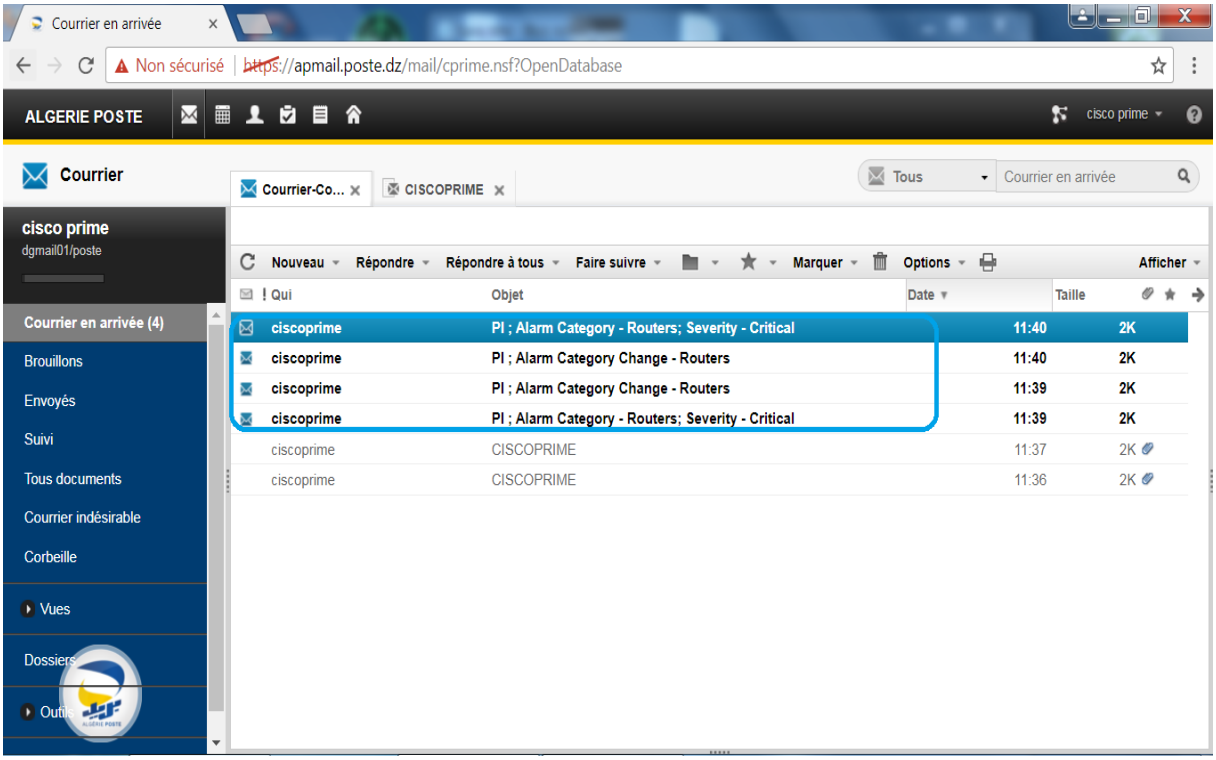


Après avoir effectué toutes les étapes, on procède maintenant à un essai pour confirmer le succès des configurations.

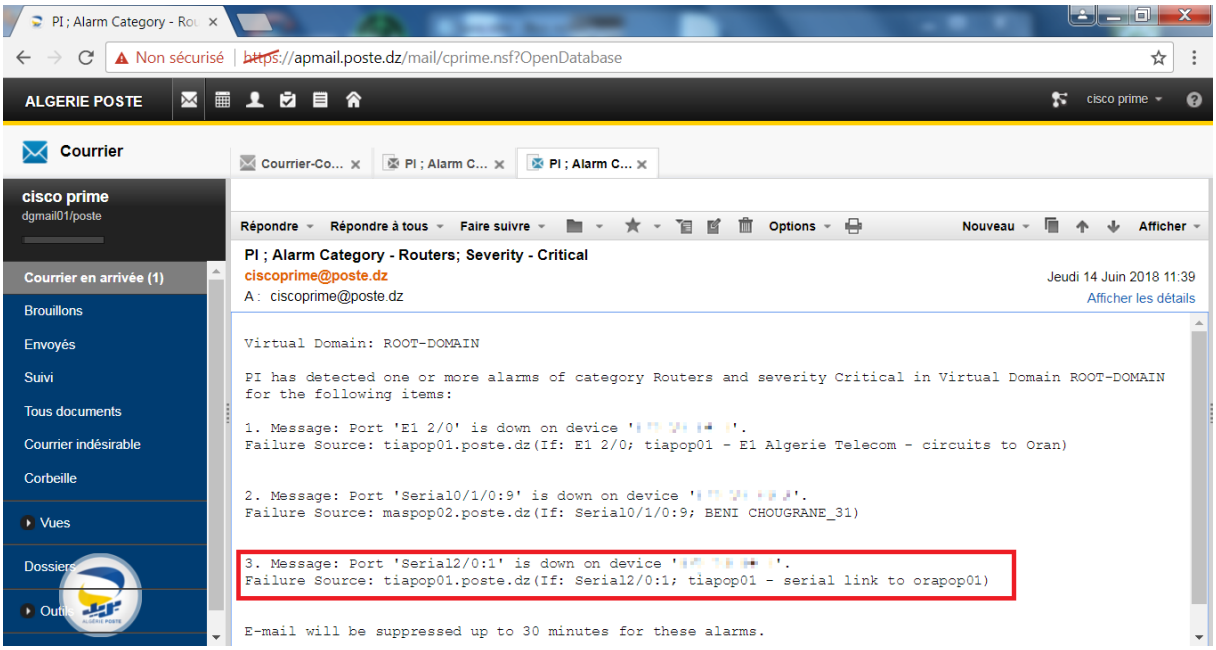
La figure ci-dessous représente un mail de test de succès des configurations précédentes.



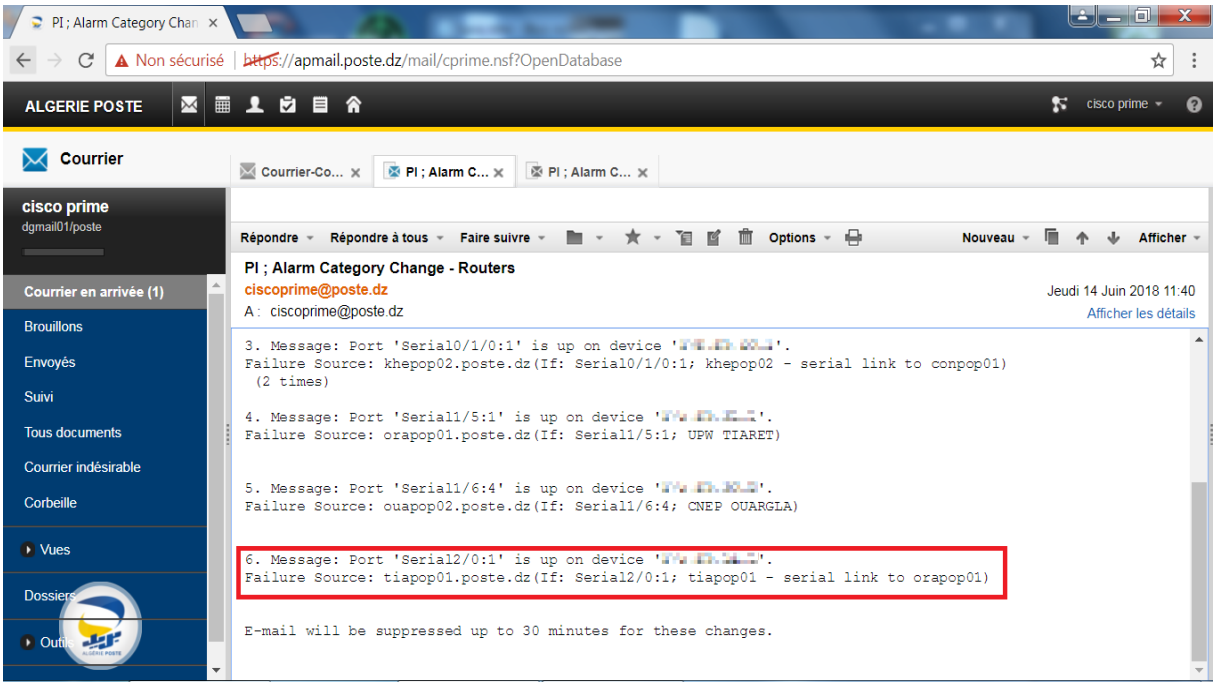
La figure ci-dessous montre la réception de notifications sous forme de mail; et cela en mentionnant le type d'événement et d'autres détails



La figure ci-dessous montre un exemple de notification envoyée sur l'état d'une des interfaces du routeur de la wilaya de Tiaret qui passe de **UP** à **Down**.



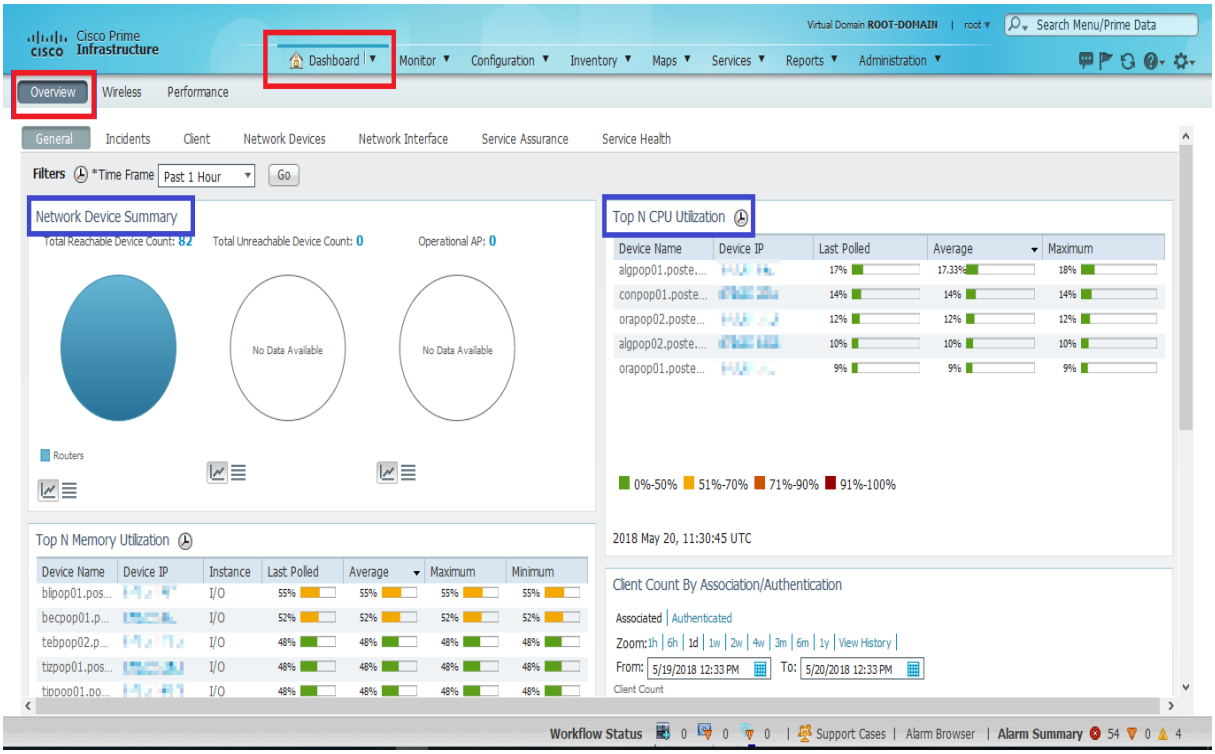
La figure ci-dessous montre une notification envoyée par mail sur l'état de l'interface du routeur de la wilaya de Tiaret qui reprend son travail en passant du statut de **Down** à celui de **Up**.



IV.4 Le Dashboard :

Après avoir configuré tous les points qu'on vient de citer, ajouté les périphériques réseaux, et ajouter les groupes de PoPs à chaque wilaya on obtient un Overview sur le Dashboard. Cet Overview donne des statistiques concernant :

- ✓ Network device summary : qui est un résumé des périphériques accessibles et non accessibles.
- ✓ Top N CPU utilization : qui est le classement des périphériques utilisant le plus de ressources en donnant des détails tels que le nom du périphérique, son adresse IP, les statistiques concernant l'interrogation du périphérique, la moyenne d'utilisation de CPU de ce dernier et enfin le maximum de CPU utilisé durant son cycle de vie.



- ✓ Top N memory utilization : qui introduit le classement les périphériques utilisant plus de mémoire que leurs voisins. Ajoutant leur noms, adresses IP, pourcentage de leurs interrogation ; le minimum, la moyenne et le maximum de la mémoire utilisée durant son cycle de vie.

  Le carré en rouge signifie l'état de la mémoire selon des couleurs :

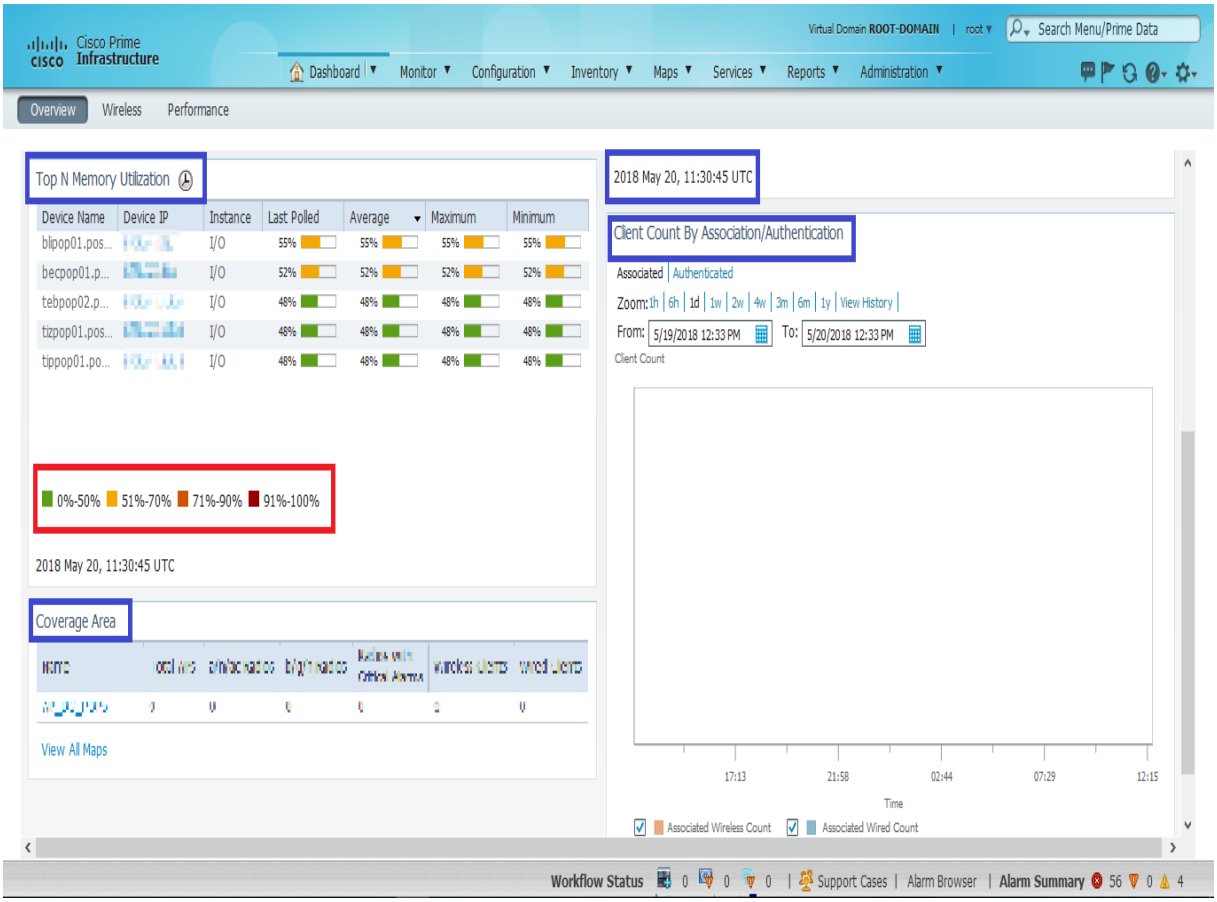
  Vert : indiquant que la mémoire utilisée est entre 0-50%.

  Orange : indiquant que l'utilisation de la mémoire est entre 51-90%.

  Rouge : indiquant un état critique de la mémoire qui est entre 91-100%.
- ✓ L'horodatage : montre la date et l'heure exacte de la dernière consultation du Dashboard pour avoir ces statistiques.
- ✓ Client count by association/authentication : affiche le nombre total de clients par association et authentification dans Prime Infrastructure sur la période sélectionnée.

  - Client associé: tous les clients connectés, qu'ils soient authentifiés ou non.

  - Client authentifié: tous les clients qui se sont connectés et ont passé les règles d'authentification, d'autorisation et autres, et sont prêts à utiliser le réseau.
- ✓ Coverge area : indiquant le nom et le nombre total des points d'accès AP, de clients filaires et sans fils ainsi que la possibilité d'avoir une map concernant ces points d'accès.



Conclusion partielle :

Dans ce chapitre nous avons traité différents aspects concernant notre outil de supervision Cisco Prime Infrastructure et ce, dans le cadre du respect des exigences du client ainsi que celles du serveur.

Nous avons procédé au déploiement de l'outil se faisant par les étapes d'installation et celles de la post-installation.

En outre cet outil présente des plusieurs fonctionnalités dont certaines n'ont pas été toutes exploitées car le besoin de l'entreprise l'exige.

Des configurations nécessaires ont été faites ;

- ajout des administrateurs en leur attribuant des droits convenables à leurs missions,
- ajout des périphériques,
- ajout des groupes,

- configuration des alarmes et des événements ainsi que la réception des notifications par mail.

Ainsi donc, le but du monitoring du réseau d'Algérie poste est atteint.

Enfin, nous avons achevé notre travail en obtenant toutes les statistiques qu'on voulait avoir pour superviser le réseau de notre entreprise. Parmi ces résultats, nous avons eu le pourcentage et l'état d'utilisation du CPU, de la mémoire, le nombre de clients par association et authentification ainsi qu'une map introduisant les PoPs se trouvant dans chaque wilaya.

Conclusion générale :

Dans ce PFE, on s'est familiariser aux concepts du monitoring des réseaux d'entreprise et en particulier à l'outil Cisco Prime Infrastructure qui fournit une solution de gestion complète pour automatiser la conception, l'exécution, l'assurance et la gestion continue des services réseau.

Pour cela, on s'est d'abord intéressé aux différents outils de supervision utilisés jusqu'à ce jour. Entre outre l'architecture et le principe de fonctionnement de la solution mis en place.

Notre travail consistait à mettre en place un outil de supervision système et réseau. Dans un premier lieu, nous avons pu étudier l'existant et dégager ses limites afin de fixer la solution retenue après l'avoir étudié. Dans la partie réalisation, nous avons mis en place l'outil Cisco Prime Infrastructure et configuré sur un serveur qualifié exécutant VMware ESXi qui utilise vSpher client pour gérer la machine virtuelle. Enfin nous l'avons configuré afin d'identifier le réseau global, pouvoir le superviser, et alerter l'administrateur par mail en cas de pannes.

L'objectif de notre projet était de permettre aux administrateurs de l'entreprise de mieux superviser les équipements et les services réseau. En effet cette solution de supervision permet de diminuer le taux de pannes lors du diagnostic et facilite les tâches de l'administrateur réseaux.

Les résultats obtenus nous ont amené à l'amélioration de ce travail par les perspectives suivantes :

- ✓ Configuration des notifications par SMS ;
- ✓ Supervision plus profonde des services réseaux et ;
- ✓ Configuration d'une map sur la carte géographique nationale regroupant toutes les régions (Est, Ouest, Centre, Sud) sur laquelle on place les périphériques principaux de chaque wilaya montrant les liens entre ces PoPs ;
- ✓ Amélioration en terme de ressources car cette version exige 16Go et 16 v CPU.

Liste des abréviations :

AES	**Advanced Encryption Standard**
AP	**Access Point**
API	**Application Programing Interface**
Bash	**Bourne-Again shell**
CPU	**Central Processing Unit**
CLI	**Command-Line Interface**
CVS	**Comma Separated Values**
CORBA	**Common Object Request Broker Architecture**
DES	**Data Encryption Stnadard**
DHCP	**Dynamic Host Configuration Prototcol**
DNS	**Domain Name System**
DRAM	**Dynamic Random-Access Memory**
ESXI	**Elastic Sky X Integrated**
FTP	**File Transfert Protocol**
FIPS	**Federal Information Processing Standards**
FCAPS	**Default Configuration Accounting Performance**
HA	**High Availability**
HDD	**Hard Disk Drive**
IP	**Internet Protocol**
ISE	**Identity Services Engine**
IWAN	**Intelligent Wan**
OSI	**Open System Interconnection model**
MIB	**Management Information Base**
MDM	**Mobile Device Management**
MSE	**Mobility Services Engine**
MTOSI	**Multi-Technology Operations Systems Interface**
MD5	**Message Digest 5**
NA	**Not Assigned**
OSS	**Operational Support System**
OVA	**Open Vertual Appliance**
RRDTool	**Round-Robin Database Tool**

POP	**Point Of Presence**
Php	**Hypertext Preprocessor**
RBAC	**Role-Based Access Control**
SSH	**Secure Shel**
SHA	**Secure Hash Algorithm**
SMTP	**Simple Mail Transfert Protocol**
SSO	**Single Sign-On**
TAC	**Technical Assistance Center**
TMF	**TeleManagement Forum**
TCP	**Transmission Control Protocol**
UDP	**User Datagram Protocol**
VPN	**Virtual Private Network VBScript (Microsoft Visual Basic Scripting Edition)**
WI-FI	**Wireless Fidelity**
WAN	**Wide Area Network**
XML	**Extensible Markup Language**

Références bibliographiques :

[1] Support de cours Généralités sur les réseaux informatiques - Dr RIAHLA Med Amine, 2008 - Consulté en Mars 2018.

[2] Implémentation d'un réseau LAN sécurisé - Mme Aicha LAABI - Institut National Spécialisé en Formation Professionnelle – El mohamadia, Mars 2013.

[3] Administration des Services Réseaux sous linux - Dr BENMOUSSA Yahia, Juin2017.

[4]https://sites.google.com/site/wwwnewtechnologiecom/reseau/reseauinformatique/terminologie-des-rseaux - Consulté en Juin 2018

[5] Etude des fonctionnalités d'un FIREWALL réseau avec un exemple d'application – Mlles Massylia OUMOHAND / Rym BOUZAD –Université M'Hamed BOUGARA –Boumerdès - 2015/2016.

[6]https://www.over-blog.com/Baie_de_stockage_definition_et_utilites-1095203942-art272288.html - Consulté en Juin 2018.

[7] http://www.o00o.org/monitoring/bases.html - Consulté en Mars 2018.

[8] Mise en place d'un outil de supervision système et réseau open source - Université Virtuelle de Tunis - Mme Abir TRABELSI, 2014/2015.

[9] http://www.frameip.com/snmp/ - Consulté en Mars 2018.

[10] http://ram-0000.developpez.com - Consulté en Mars 2018.

[11] www.cisco.com - Consulté en Mars 2018.

[12]https://www.cisco.com/c/dam/en/us/products/cloud-systems-management/prime_architecture_wp.pdf - Consulté en Mars 2018.

[13] https://zen.systems/network-monitoring/ - Consulté en Mai 2018

[14] http://tomwiki.wikidot.com/wiki:le-protocole-snmp - Consulté en Mai 2018

[15]http://world-connect.ch/services-informatique/monitoring/ - Consulté en Juin 2018.

[16] https://www.ip-label.fr - Conuslté en Juin 2018.

ANNEXE :

A

AES: est un algorithme de chiffrement par blocs à clé symétrique et un standard gouvernemental américain pour le chiffrement et le décryptage sécurisés et classifiés des données.

Apache : est un serveur HTTP créé et maintenu au sein de la fondation Apache. C'est le serveur HTTP le plus populaire du World Wide Web.

API : est un ensemble de définitions de sous-programmes, de protocoles et d'outils pour la création de logiciels d'application. En termes généraux, il s'agit d'un ensemble de méthodes de communication clairement définies entre différents composants logiciels. API facilite le développement d'un programme informatique en fournissant tous les blocs de construction, qui sont ensuite assemblés par le programmeur.

AP : est un périphérique matériel réseau qui permet à un périphérique Wi-Fi de se connecter à un réseau câblé.

Ajax : ensemble de technique de développement web utilisant de nombreuses technologies web coté client pour créer des applications web.

B

Bash : est un interpréteur en ligne de commande de type script. C'est le shell Unix du projet GNU.

C

CACTID : un moteur de récolte des données en C, utilisant avantageusement les Threads POSIX

CPU : est la partie d'un système informatique communément appelé «cerveau» d'un ordinateur. Le processeur est responsable de l'exécution d'une séquence d'instructions stockées appelée programme.

Cisco WebEx : est une entreprise qui fournit des applications de collaboration à la demande, de réunion en ligne, de conférence Web et de vidéoconférence

Cisco Jabber : est une nouvelle application de communications unifiées. Cisco Jabber permet d'accéder à la présence, à la messagerie instantanée (IM), à la voix, à la vidéo, à la messagerie vocale, au partage de bureau et à la conférence.

CLI : un est interpréteur de langage de commande ou shell (informatique), permet d'interagir avec un programme informatique où l'utilisateur émet des commandes au programme sous la forme de lignes de texte successives (lignes de commande).

CVS : est un fichier de valeurs séparées par des virgules qui permet d'enregistrer les données dans un format structuré de table. Les fichiers CSV ressemblent à une feuille de calcul de type Excel mais avec une extension .csv. Traditionnellement, ils prennent la forme d'un fichier texte contenant des informations séparées par des virgules, d'où le nom.

CORBA : est une norme définie par le groupe OMG (Object Management Group) conçu pour faciliter la communication des systèmes déployés sur diverses plates-formes

D

DES : est une norme commune pour le cryptage des données et une forme de cryptographie à clé secrète (SKC), qui utilise une seule clé pour le cryptage et le décryptage. La cryptographie à clé publique (PKC) utilise deux clés, à savoir une pour le cryptage et une pour le déchiffrement.

DHCP : est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.

DNS : est un protocole indispensable au fonctionnement d'Internet. Il permet la résolution des noms de domaines qui consiste à assurer la conversion entre les noms d'hôtes et les adresses IP.

Débit Disk I/O : c'est la vitesse avec laquelle le transfert de données a lieu entre le disque dur et la RAM. Il mesure les Entrées / Sorties du disque actif

DRAM : est un type de mémoire à semi-conducteur à accès aléatoire qui stocke chaque bit de données dans un condensateur minuscule séparé dans un circuit intégré. Le condensateur peut être chargé ou déchargé ; ces deux états sont pris pour représenter les deux valeurs d'un bit, classiquement appelées 0 et 1.

E

ESXI : est une plate-forme de virtualisation de serveur VMware permet de déployer et servir des ordinateurs virtuels.

F

FTP : est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet depuis n ordinateur de copier des fichiers vers un autre ordinateur, d'alimenter un site web, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

FCAPS : est un modèle et un cadre du réseau de gestion des télécommunications ISO pour la gestion de réseau. FCAPS est un acronyme de défaut, configuration, comptabilité, performance, sécurité,

FIPS : Normes fédérales de traitement de l'information sont des lignes directrices et des spécifications publiées par l'Institut national des normes et de la technologie (NIST) qui s'appliquent aux systèmes informatiques fédéraux**.**

H

HA : est une caractéristique d'un système qui vise à garantir un niveau de performance opérationnelle convenu, généralement en temps de fonctionnement, pour une période supérieure à la normale. Deux moyens complémentaires sont utilisés pour améliorer la haute disponibilité :

- la mise en place d'une infrastructure matérielle spécialisée, généralement en se basant sur de la redondance matérielle.
- la mise en place de processus adaptés permettant de réduire les erreurs, et d'accélérer la reprise en cas d'erreur.

HDD : est le mécanisme qui contrôle le positionnement, la lecture et l'écriture du disque dur, qui fournit le stockage des données. Les disques durs se trouvent dans les ordinateurs de bureau, les appareils mobiles, l'électronique grand public et les baies de stockage d'entreprise dans les centres de données.

I

IP : est une famille de protocole de communication de réseau informatique conçus pour utiliser par internet.

ISE : est un produit d'administration réseau qui permet la création et l'application de stratégies de sécurité et d'accès pour les périphériques d'extrémité connectés aux routeurs et

commutateurs de l'entreprise. Le but est de simplifier la gestion des identités entre divers appareils et applications.

IWAN : est un système qui améliore la collaboration et les performances des applications cloud tout en réduisant les coûts d'exploitation du WAN. La solution IWAN fournit des conseils de conception et de mise en œuvre aux entreprises souhaitant déployer un WAN indépendant du transport avec un contrôle intelligent du chemin, une optimisation des applications et une connectivité sécurisée vers Internet et les succursales tout en réduisant les coûts d'exploitation du WAN.

M

Modèle OSI (Open System Interconnection model) : est un standard de communication, en réseau, de tous les systèmes informatiques. C'est un modèle de communications entre ordinateurs proposé par l'ISO (Organisation Internationale de Normalisation) qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

Modèle TCP/IP : est l'ensemble des protocoles utilisés pour le transfert des données sur Internet. C'est une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante

MIB : Base d'information pour la gestion du réseau) est un ensemble d'informations structuré sur une entité réseau, par exemple un routeur, un commutateur ou un serveur. Ces informations peuvent être récupérées, ou parfois modifiées, par un protocole comme SNMP.

MDM : est un terme de l'industrie pour l'administration des appareils mobiles, tels que les smartphones, les tablettes électroniques, les ordinateurs portables et les ordinateurs de bureau. MDM est généralement mis en œuvre avec l'utilisation d'un produit tiers qui a des fonctionnalités de gestion pour les fournisseurs particuliers de périphériques mobiles.

MSE : est un appareil ou moteur matériel qui utilise des données collectées par une appliance Cisco pour des tâches telles que la détection radio malveillante, et le partage avec des applications Cisco haut de gamme et des applications tierces pour la sécurité, le contrôle d'accès et la gestion de réseau. MSE est conçu pour décharger le traitement des applications d'un périphérique dédié, créant ce que les dirigeants de Cisco appellent un «avion de services».

MTOSI: est une norme pour la mise en œuvre d'interfaces entre OSS. Les fournisseurs de services (opérateurs) utilisent plusieurs systèmes de support opérationnel (OSS) pour gérer

des réseaux complexes. Puisque les différentes parties du réseau doivent interagir, les OSS doivent également interagir.

MD5: est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier (ou bien un message).

O

OSS : Un système de support opérationnel est un groupe de programmes informatiques ou un système informatique utilisé par les fournisseurs de services de communications pour surveiller, contrôler, analyser et gérer un ordinateur ou un système de réseau téléphonique.

OVA : Il s'agit d'un package qui contient des fichiers utilisés pour décrire une machine virtuelle, qui inclut un fichier descripteur .OVF, un fichier manifeste facultatif (.MF) et des fichiers de certificat, ainsi que d'autres fichiers associés.

P

PoP : est un point de démarcation artificiel ou un point d'interface entre entités communicantes. ... Un point de présence Internet héberge généralement des serveurs, des routeurs, des commutateurs réseau, des multiplexeurs et d'autres équipements d'interface réseau. Il est généralement situé dans un centre de données.

Php : est un langage de programmation libre, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. PHP est un langage impératif orienté objet.

Perl : est un langage de programmation permet de traiter facilement de l'information de type textuel. Ce langage, interprété, s'inspire des structures de contrôle et d'impression du langage C, mais aussi de langages de scripts sed, awk et shell (sh).

Il prend en charge les expressions régulières dans sa syntaxe même, permettant ainsi directement des actions sur l'aspect général de séquences de texte.

R

RBAC : le contrôle d'accès basé sur les rôles (RBAC) est une approche visant à restreindre l'accès du système aux utilisateurs autorisés.

RRDTool : est un outil de gestion de base de données, utilisé par de nombreux outils open source, tels que Cacti et Nagios, pour la sauvegarde de données cycliques et le tracé de graphiques, de données chronologiques. Cet outil a été créé pour superviser des données

serveur, telles la bande passante et la température d'un processeur. Le principal avantage d'une base RRD est sa taille fixe

S

SSH : est à la fois un programme informatique et un protocole de communication sécurisé. Il impose un échange de clés de chiffrement au début de connexion, par la suite toutes les trames sont chiffrées. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.

SHA : est un algorithme de hachage cryptographique qui prend une entrée et produit une valeur de hachage de 160bits (20octets), généralement rendue sous la forme d'un nombre hexadécimal de 40 chiffres.

SMTP : est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique.

SSO : est un service d'authentification de session et d'utilisateur qui permet à un utilisateur d'utiliser un ensemble d'informations d'identification de connexion (par exemple, nom et mot de passe) pour accéder à plusieurs applications.

T

TAC : est un département au sein d'une entreprise dont l'objectif principal est le réseautage, ou un fournisseur de services Internet. Le TAC travaille également en étroite collaboration avec le Network Operations Center d'une société. Un TAC peut uniquement surveiller les éléments avec un signal de retour, tel qu'un modem

TCP : est le principal protocole réseau utilisé par les connexions Internet. C'est un protocole de transport au même titre que l'UDP sauf qu'il travaille en mode connecté. Les données transmises sont donc vérifiées. Dans le modèle TCP/IP, il est entre la couche de transport (généralement IP) et la couche application.

TELNET : est un protocole standard d'Internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de base pour permettre de relier un client (système composé d'un affichage et d'un clavier) à un interpréteur de commande (côté serveur).

TMF : est une association industrielle mondiale qui conduit la transformation numérique de l'industrie des communications grâce à la collaboration.

U

UDP : est un des principaux protocoles de télécommunication utilisés par internet .Il fait partie de la couche transport de la pile de protocoles TCP/IP dans l'adaptation approximative de cette dernière au modèle OSI, il appartiendrait à la couche 4, comme TCP

V

VPN : est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local .Il correspond en fait à une interconnexion de réseaux locaux via une technique de tunnel.

VBScript : est un sous-ensemble de Visual Basic utilisé en tant que langage de script d'usage général. Il est souvent comparé au JScript.

Vmware server : est un produit de virtualisation qui permet de partitionner un seul serveur physique en plusieurs machines virtuelles. Le serveur VMware fonctionne avec Windows,Linux et Netware, dont tout ou partie peut être utilisé simultanément sur le même matériel

Vsphere client : est une suite de produits, utilisé pour installer et gérer des machines virtuelles via l'hyperviseur ESXi et VMware.

W

WI-FI : est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11 (ISO/CEI 8802-11). Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, modem Internet, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux.

WAN : c'est un réseau à l'échelle d'un pays, généralement celui des opérateurs. Le plus connu des WAN est Internet.

X

XML : est un format universel maintenu par le W3C utilisé pour la représentation et le transfert de données structurées sur le web ou entre différentes applications**.**