Amélioration des contrôles d'accès aux équipements LAN dans le cadre de la télé-administration des matériels

Florian Goulais

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE REGIONAL ASSOCIE DE BRETAGNE

_____

MEMOIRE

présenté en vue d'obtenir

le DIPLOME d'INGENIEUR CNAM

SPECIALITE : Architecture et Ingénierie des Systèmes et des Logiciels

OPTION : Intégration et ingénierie de systèmes

par

GOULAIS, Florian

_____

Amélioration des contrôles d'accès aux équipements LAN dans le cadre de la télé-administration des matériels

Soutenu le 31 janvier 2014

_____

JURY

PRESIDENT : **Professeur Yann POLLET**

MEMBRES : **M. Eric BORNETTE**

M. VIDAL Jean-Marc

M. Ronan LEBEHEREC

M. Eric DUPUIS

Remerciements

Je remercie ma hiérarchie et en tout premier lieu le colonel MOTUEL qui m'a permis de réaliser mon mémoire sur un projet au profit du CIRISI. Je tiens à remercier également le commandant GONIDEC, l'IEF GAUTRAIS et le Lieutenant LAMY qui m'ont soutenu dans cette démarche.

Enfin, je souhaite particulièrement remercier ceux qui m'ont apporté leur soutien, leur aide et leurs connaissances pour la réalisation de ce projet : M. Eric BORNETTE, le commandant VIDAL, M. Ronan LEBEHEREC, l'adjudant-chef CAÏTUCOLI, l'adjudant-chef DE CRECY et son équipe ainsi que Maëlle.

Sommaire

CONTENU

I INTRODUCTION

Le projet traité dans ce mémoire concerne l'implémentation d'une solution d'authentification centralisée sur des éléments actifs réseaux.

C'est un projet que j'ai mené entre 2012 et 2013 au sein de la structure qui m'emploie.

Ce sujet est fortement lié aux évolutions passées et futures de la structure cliente et aux évolutions technologiques. Tant au niveau organisationnel que fonctionnel, il est important de bien appréhender le contexte dans lequel s'inscrit le projet. Ce sont les évolutions structurelles et techniques qui ont induit la mise en place d'une solution d'authentification réseaux sécurisée et centralisée sur le parc d'éléments actifs.

Ce mémoire suit la chronologie du projet et traite de l'ensemble de ses étapes ayant jalonnées sa réalisation.

Après la présentation du contexte, les phases d'étude du besoin, de conception et de réalisation seront plus particulièrement développées.

1 LE CIRISI

En 2009, suite à la révision générale des politiques publiques (*RGPP*) et la diffusion du livre blanc sur la défense nationale, le ministère de la défense a fortement évolué. La fonction soutien des organismes de la défense a initié la rationalisation de ses ressources.

Ainsi les divers services informatiques de proximité se sont vus mutualisés et intégrés au sein de centres de service : **Les CIRISI** (*Centre Inter-armées des Réseaux d'Infrastructure et des Systèmes d'Information*). Il existe à l'heure actuelle 38 CIRISI en France, auxquels sont rattachés 117 détachements. Ils sont tous subordonnés à 7 DIRISI locales réparties sur l'ensemble du territoire métropolitain.

Le CIRISI Rennes a été créé le premier janvier 2009. Cependant ce n'est qu'en 2010 qu'il intègre les services locaux d'aide aux usagers et agrandit ainsi ses prérogatives pour exister sous sa forme actuelle.

Il est principalement composé des éléments issus des entités militaires rattachées au bassin Rennais (Côtes d'Armor, Morbihan, Ille et Vilaine et Mayenne) et dépend organiquement de la DIRISI Rennes.

Son organisation, ses ressources et ses missions seront présentées dans les parties suivantes.

1.1 L'ORGANISATION DU CIRISI

1.1.1 AU SEIN DU MINISTERE DE LA DEFENSE

Comme son nom l'indique, la DIRISI (Direction **Inter-armées** des Réseaux d'Infrastructure et des Systèmes d'Information) a toujours eu une vocation inter-armées au sein du ministère de la défense. C'est donc naturellement que suite aux réorganisations de 2010, la chaîne DIRISI a gagné en compétence avec l'intégration des CIRISI comme l'indique la figure 1.

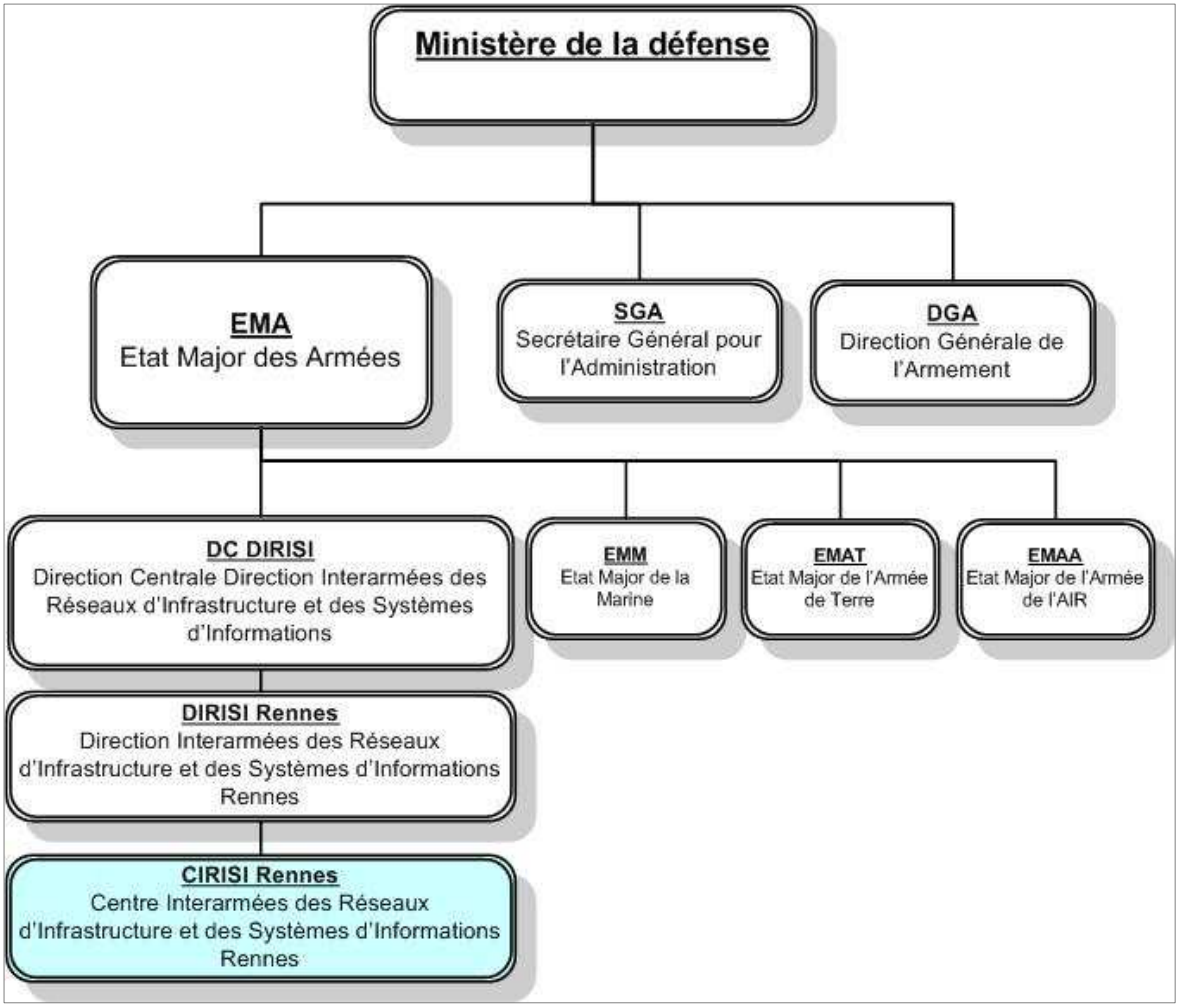


Figure 1 : Positionnement hiérarchique du CIRISI Rennes au sein du ministère de la défense

1.1.2 L'ORGANISATION INTERNE

Comme le décrit la figure 2 ci-dessous, le CIRISI Rennes est composé d'un commandement, d'une conduite d'activité ainsi que de six divisions ou cellules ayant un champ de compétence zonal ou technique.

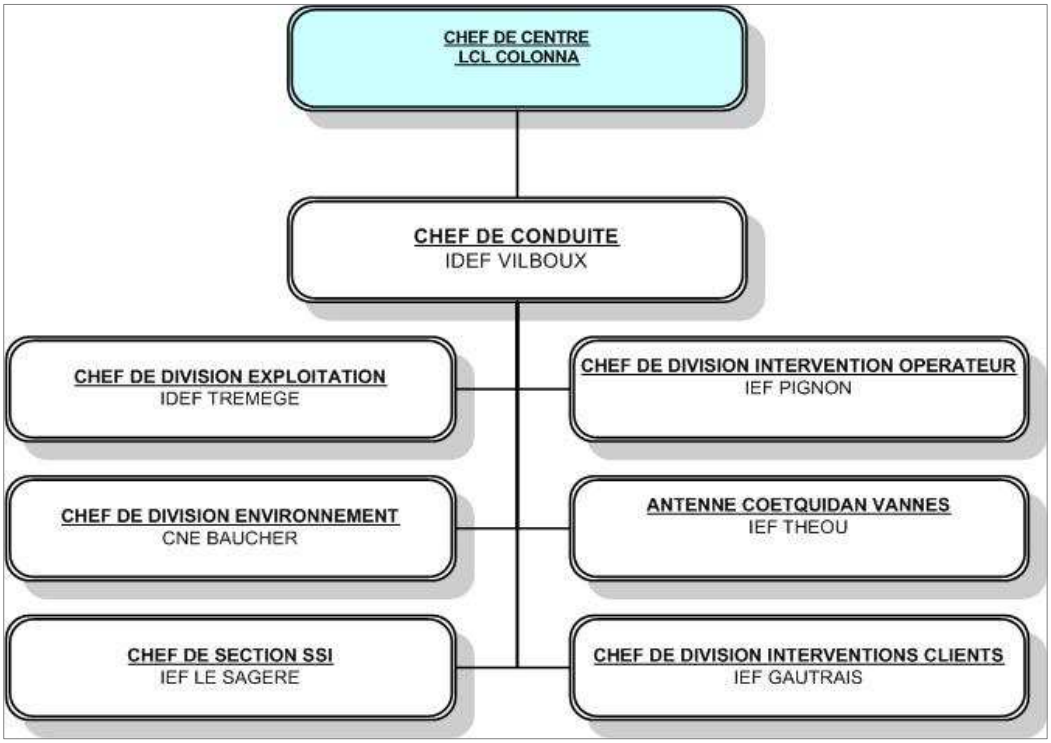


Figure 2 : Organigramme interne du CIRISI

La **division environnement (DEV)** assure le « soutien de l'homme » et notamment les fonctions RH (*Ressources Humaines*) et logistiques.

La **section SSI** est responsable de tous les aspects liés à la SSI (audit, sensibilisation, veille).

La **division intervention opérateur** (DIO) a à sa charge le brassage et le maintien en conditions opérationnelles de la desserte téléphonique et réseaux.

La **division intervention clients (DIC)** intervient auprès des utilisateurs finaux et notamment sur les postes clients.

L'**antenne de COETQUIDAN / VANNES** assure les missions de la DIC mais aussi une partie des missions de la DIO pour les sites distants de Cöetquidan et Vannes.

Enfin, la **division exploitation (DEX)** a pour mission d'assurer l'hébergement et l'exploitation des systèmes d'informations ainsi que l'exploitation des réseaux locaux.

Les WAN (*Wide Area Network, réseaux étendu de transport*) quant à eux sont gérés au niveau national.

La cellule « Réseaux » de la division exploitation (*DEX/RZO*) s'occupe plus particulièrement de l'administration des EAR (*Equipements Actifs Réseau*), l'expertise et l'audit réseau ainsi que la configuration de l'outil de supervision (HP OpenView).

Cette cellule est le client direct du projet que j'ai mené.

1.2 LES RESSOURCES : EFFECTIFS / EMPRISES GEOGRAPHIQUES / MOYENS

En termes d'effectifs, le CIRISI Rennes est composé de 162 personnels (civil et militaires confondus) répartis sur « 7 » sites.

Comme le présente la figure 3, sa zone de responsabilité s'étend sur les quatre départements des Côtes d'Armor, du Morbihan, de l'Ille et Vilaine et de la Mayenne. Cela représente 22 emprises géographiques de tailles et de compositions différentes (volume du parc soutenu, étendue et complexité du réseau, nécessité du maintien en conditions opérationnelles, etc…).

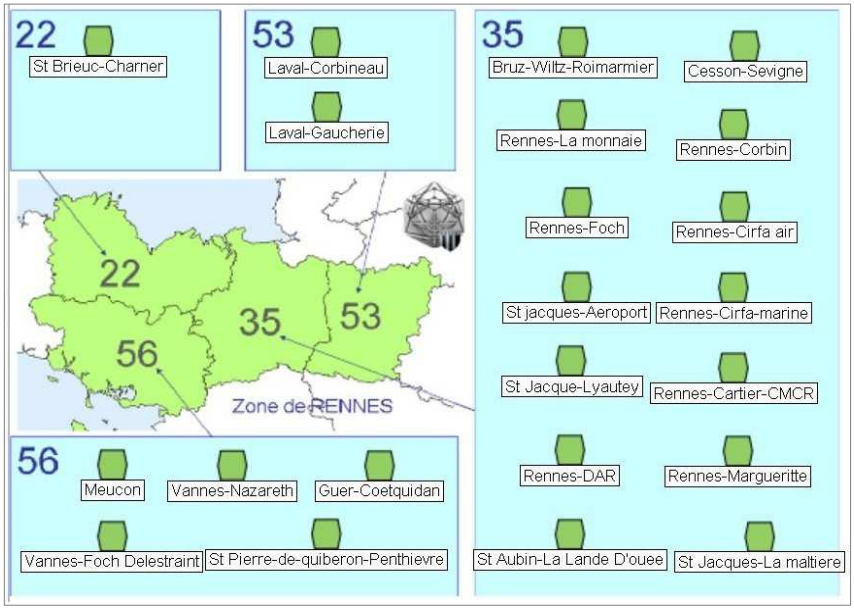


Figure 3 : Zone de responsabilité du CIRISI Rennes

1.3 LES MISSIONS DU CIRISI

Tous les CIRISI ont les mêmes missions. En tant que centre de service au profit des entités soutenues, ils doivent :

- Assurer la continuité et la disponibilité des SIC (*Systèmes d'Information et de Communication*) ;
- Participer à la réalisation et aux déploiements des projets SIC ;
- Mettre en place et assurer le soutien des SIC de circonstance ;
- Assurer la liaison et le conseil avec les formations de rattachement ;
- Participer à la gestion des ACSSI (*Article Contrôlés pour la Sécurité des Systèmes d'Information)*;
- Participer à la gestion des biens de l'opérateur et des formations ;

Les unités soutenues disposent d'un contrat de service adapté à leurs besoins négocié avec la DIRISI Rennes qu'elles peuvent bien évidemment renégocier en fonction de l'évolution des missions opérationnelles.

Le CIRISI Rennes, gère et soutient près de 9000 abonnés téléphoniques et 7000 postes informatiques. Cela correspond à un volume de plus de 2800 interventions curatives et 9000 petites installations par an.

Par ailleurs, il dispose d'une surface de stockage d'environ 2000 m² et est chargé de l'élimination de 90 tonnes d'équipement électrique et électronique (DEEE) par an.

Un point particulier concerne la cellule DEX/RZO. En effet, comme le représente la figure 4, la DIRISI Rennes a décidé de mutualiser les zones de responsabilités des cellules DEX/RZO de l'ensemble des CIRISI sous sa responsabilité (Rennes, Tour, Orléans, Avord et Evreux)

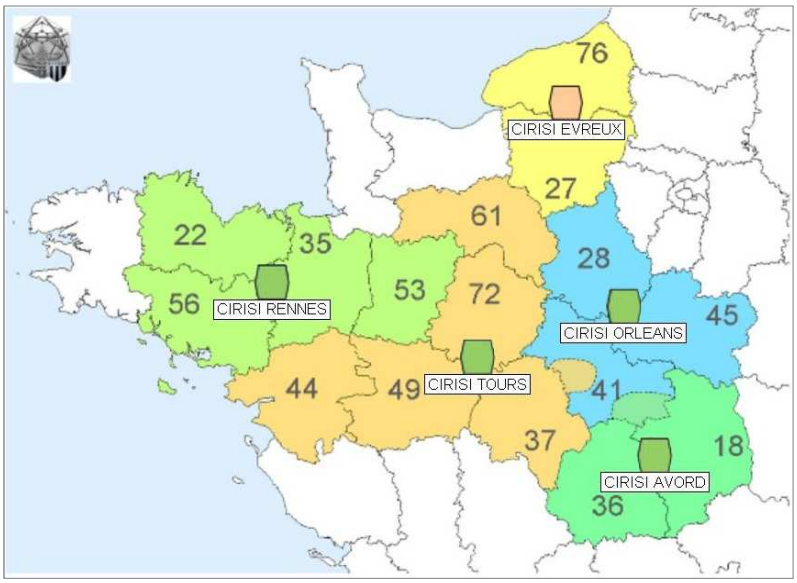


Figure 4 : Zone de responsabilité des DEX/RZO de la DIRISI Rennes

Ainsi, chacune des 5 cellules a autorité pour intervenir sur l'ensemble de la zone de responsabilité de la DIRSI Rennes. Cependant la tendance actuelle vise à réduire le nombre de personnels en mutualisant les missions. Ce contexte est détaillé ci-après.

2 LE CONTEXTE DU PROJET

2.1.1 SITUATION ET CONTEXTE LOCAL

Décidée en 2007, la révision générale des politiques publiques a visé à remettre à plat l'organisation de la fonction publique, via notamment le non-remplacement d'un fonctionnaire sur deux partant à la retraite.

La chaîne DIRISI est une des composantes principales de la fonction soutien (des systèmes d'informations) du ministère de la défense. Elle a donc été impactée fortement par les réorganisations opérées. Ses effectifs ont diminué alors que ses missions ont évolué.

Celles-ci, couvrant entre autres l'exploitation des SI, leur maintien en conditions opérationnelles et l'application des contraintes de sécurité exigent beaucoup de personnels et de temps ce qui induit un coût important.

Les mutations opérées au sein de la chaîne DIRISI tant au niveau RH que fonctionnels nécessitent d'adapter les outils actuels mis à disposition des équipes techniques. En effet, depuis 2010 un processus de mutualisation et de rationalisation a été initié. Il est donc nécessaire de disposer des outils adéquats afin de s'adapter à ce nouvel environnement.

2.1.2 LES TENDANCES ET EVOLUTIONS

Vis à vis de l'administration réseau, la mutation du CIRISI en centre de services va impliquer la mise en place de nouvelles fonctionnalités. En effet les personnels de ce dernier devront avoir la possibilité d'intervenir à distance sur les EAR avec des droits limités.

De plus, les diverses cellule DEX/RZO de la DIRISI Rennes vont, à terme, être physiquement regroupées sur Rennes. Leurs zones de responsabilités et leurs missions se verront redéfinies afin d'être mutualisées.

Enfin, la Direction Centrale de la DIRISI (DC DIRISI) étudie la mise en place de plusieurs Centre Nationaux de Mise en Œuvre Réseaux qui se répartiront la supervision et l'exploitation de l'ensemble du territoire Français.

La tendance générale est donc à la mutualisation des compétences, la réduction des effectifs et l'élargissement des zones de responsabilités. Ce changement de mode de fonctionnement va nécessiter de faire évoluer les outils actuels afin de correspondre aux nouvelles contraintes de coûts et de mobilité. Le contexte est donc un élément fondamental du projet décrit ci-dessous.

3 LE PROJET

3.1.1 INTERVENANTS ET ROLES

En premier lieu, j'aurais la responsabilité de la réalisation du projet (étude, conception et réalisation). L'ensemble de ces étapes sera entièrement réalisé par mes soins sans délégation.

Le projet sera mené en collaboration étroite avec la Cellule DEX/RZO, cliente du projet.

Le CDT VIDAL, chef de la « conduite des interventions » au sein de la Division Exploitation, apportera son soutien notamment dans l'analyse de risque et sera le tuteur entreprise.

3.1.2 OBJECTIFS DU PROJET

Le projet mené doit répondre impérativement aux objectifs suivants. Ils sont de trois ordres différents :

Fonctionnels :

Le projet doit apporter une solution pleinement fonctionnelle permettant à une équipe restreinte (environ 20 personnels) d'administrer l'ensemble des EAR cibles (environ 900). Cette solution doit permettre la délégation à une structure, telle que le service desk (SDK), de tout ou partie des fonctions d'administration et/ou d'exploitation.

Économiques :

La solution de télé-administration doit réduire le temps actuel d'exploitation et d'administration des EAR et ainsi permettre de réaliser une économie par rapport au mode de fonctionnement initial. Cet objectif est fortement lié aux restructurations actuelles de la chaîne soutien du ministère de la défense.

Sécuritaires :

Une analyse de risque devra être effectuée sur la partie Télé-administration. Celle-ci mettra en relief les éléments de sécurité à prendre en compte et définira les objectifs de sécurité auxquels la solution implémentée devra répondre.

Par ailleurs, il doit aussi prendre en compte nombre de contrainte. Cette partie sera plus amplement traitée dans la partie **II ETUDE DES BESOINS** (page 16).

3.1.3 COMPOSANTES

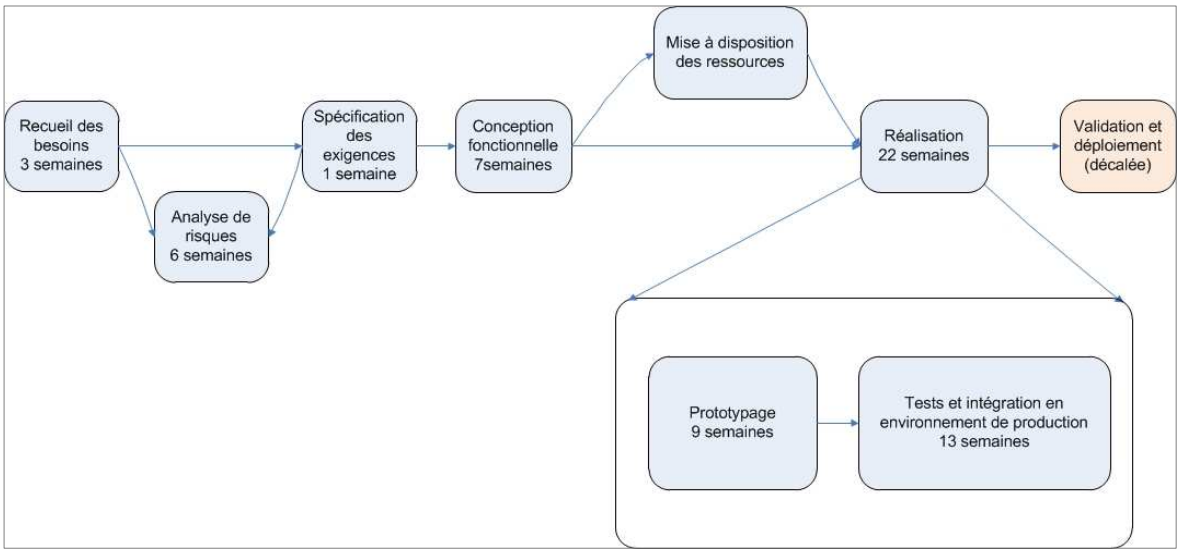
Le projet vise à implémenter une solution de télé-administration des EAR. La solution retenue devra prendre en compte l'existant afin d'intégrer la solution de manière cohérente.

En l'occurrence, la base d'annuaire des utilisateurs, le parc d'EAR ainsi que la configuration des stations de travail des utilisateurs et des administrateurs seront des éléments prédéterminés.

Ce point sera détaillé plus amplement dans la partie **III CONCEPTION** (page 23).

3.1.4 DEROULEMENT DU PROJET

Le projet suivra un cycle traditionnel d'ingénierie avec un prototypage préalable.



Étant seul à travailler sur ce projet, la responsabilité de l'ensemble des tâches m'a été dévolue.

Plus spécifiquement, la partie réalisation sera gérée selon une méthode itérative qui apporte le bénéfice d'une plus grande souplesse dans sa gestion et permet de mieux associer le client à la phase de conception.

Ce point sera particulièrement décrit à la partie **IV REALISATION** (page 34).

II ETUDE DES BESOINS

L'étude du besoin de ce projet consiste en l'analyse de l'existant, l'analyse de risque de la fonction télé-administration ainsi que le recueil des besoins. Les éléments ainsi obtenus vont permettre de spécifier techniquement le besoins sous la forme d'un cahier des charges qui servira lors de la recette du projet.

1 ANALYSE DE L'EXISTANT

1.1 REPARTITION DES ÉQUIPEMENTS ACTIFS RESEAUX

La cellule DEX/RZO gère actuellement plus de 900 EAR (ou « pile » d'EAR). Ce parc est hétérogène et compte 42 modèles d'équipement différents et 7 marques. Ceux-ci sont répartis sur l'ensemble des CIRISI Rennes, Avord, Orléans et Tours. Le CIRISI d'Evreux constitue une particularité car il n'est, pour l'instant, pas managé par le CIRISI Rennes. Avec la tendance aux regroupements des services et à la mutualisation des ressources il est fort probable que cela évolue dans l'avenir. La figure 5 montre la répartition des éléments actifs.

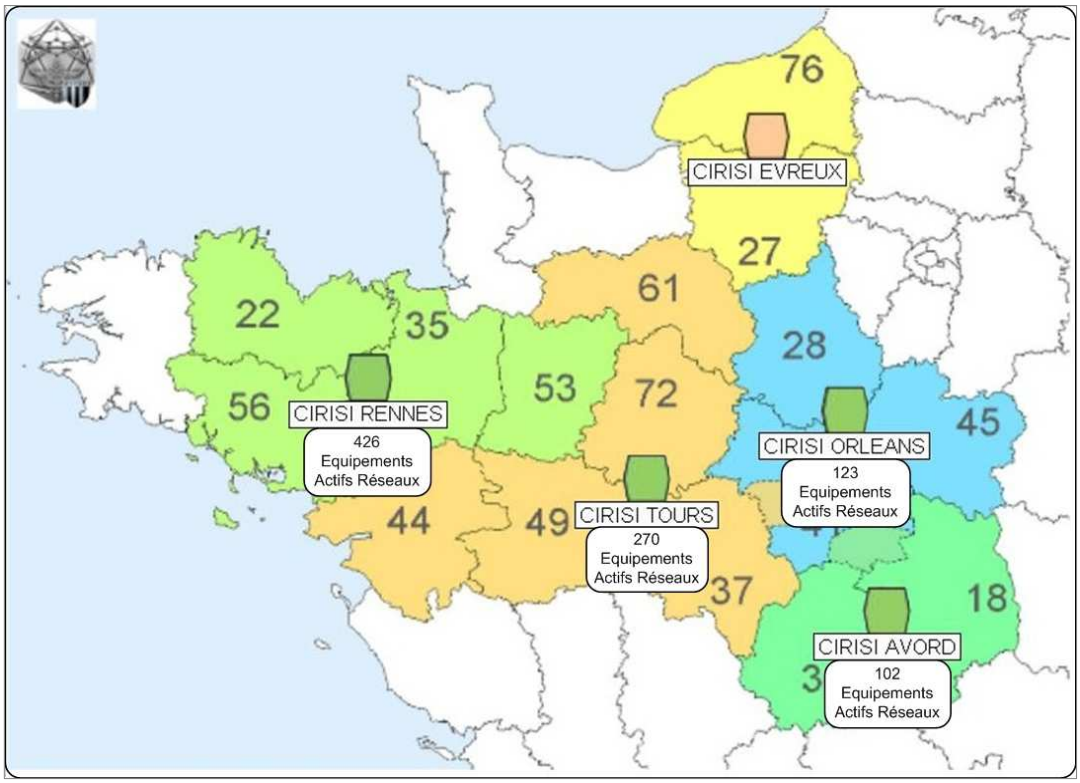


Figure 5 : répartition des EAR gérés

1.2 REPORTING

Pour monitorer l'ensemble de ces EAR, la cellule DEX/RZO utilise actuellement le produit « HP Node Network Manager ». Il offre un reporting très précis et modulable. En effet celui-ci s'appuie sur le protocole SNMP (*Simple Network Management Protocole*).

Ce protocole permet, en théorie, de manager les équipements actifs à distance. Cependant il n'offre pas de fonctionnalité d'authentification suffisante pour les besoins du projet. Ce produit ne répond donc pas aux exigences de sécurité en vigueur.

1.3 ADMINISTRATION

Pour ce qui concerne l'administration des EAR, deux possibilités s'offrent au technicien :

- L'administration locale ;
- L'administration à distance ;

Ces modes d'administration sont présentés ci-après.

Comme le détaille la figure 6 ci-dessous, dans le cas de l'administration locale, l'administrateur doit être physiquement à proximité de l'équipement à manager. Il se connecte à celui-ci via le port console. L'authentification est faite localement.

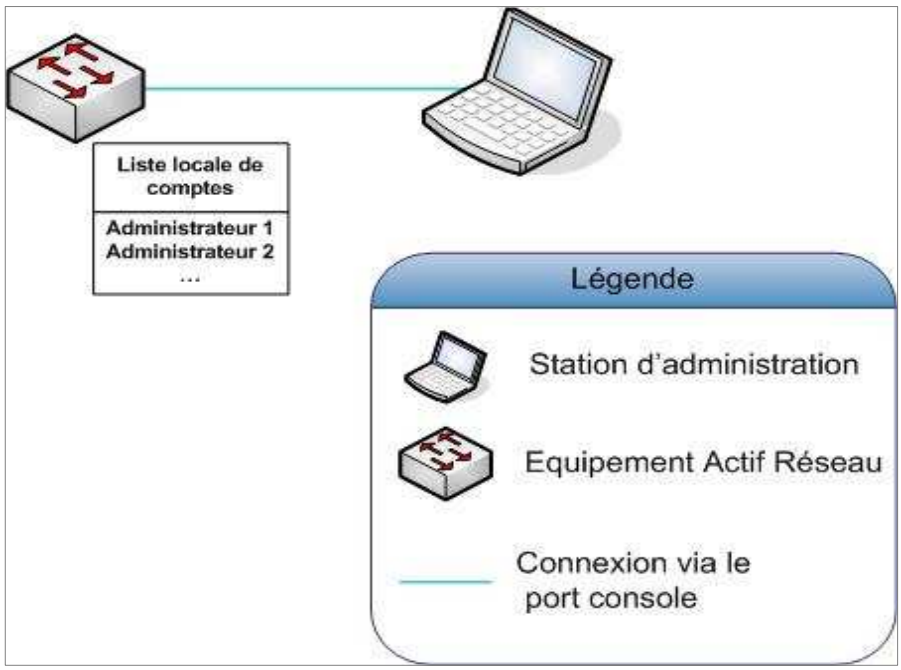


Figure 6 : authentification locale à un EAR

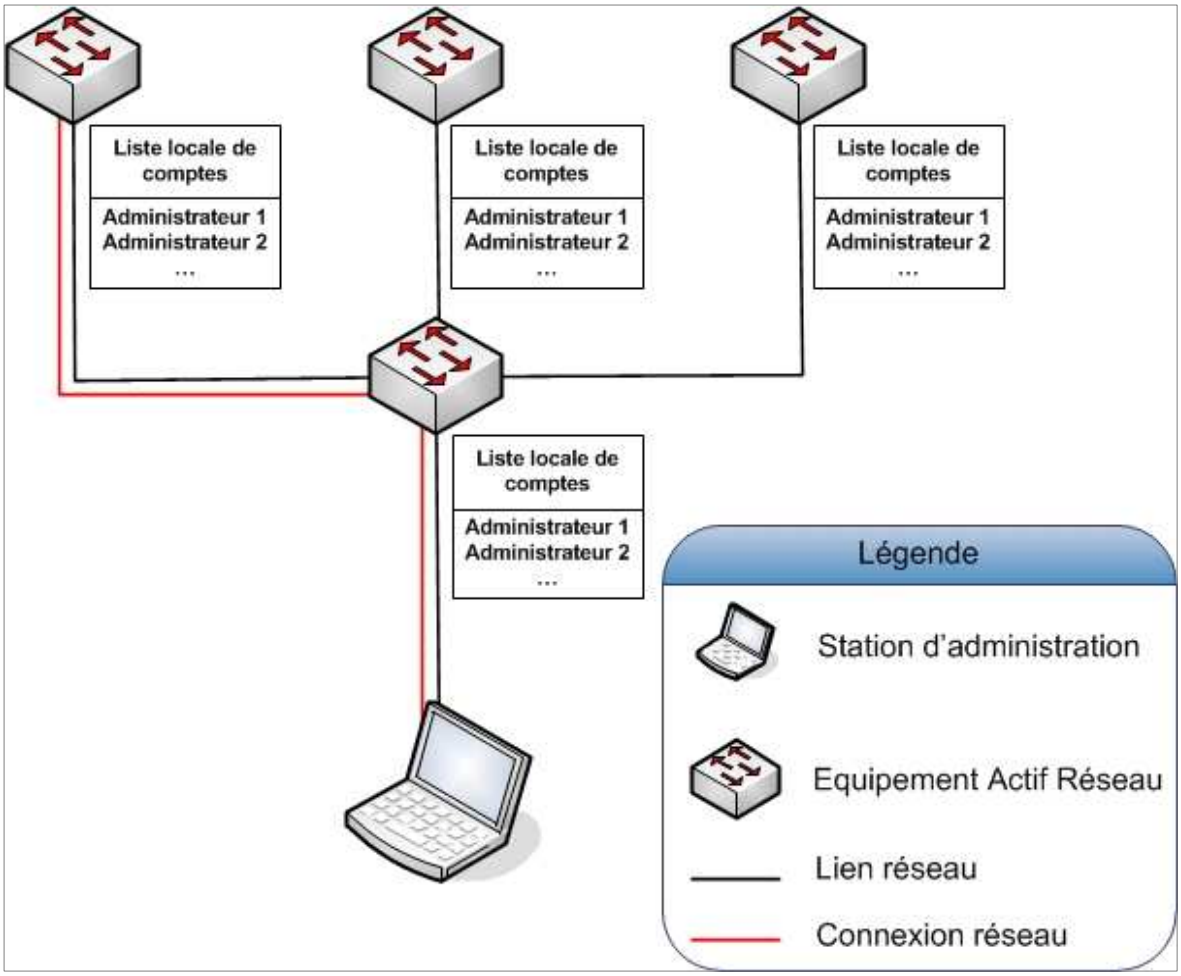


Figure 7 : authentification à distance sur un EAR

Par contre, comme le présente la figure 7 ci-dessus, lorsque l'administration se fait à distance, elle s'appuie sur une connexion réseau. Cependant, l'authentification de l'administrateur se fait de la même manière que précédemment : par rapport à une base de comptes locale. Ainsi chaque base de compte est propre à un équipement.

Les mots de passe des équipements sont changés régulièrement et stockés dans une base de données cryptée.

La modification des comptes et/ou mots de passe est une action coûteuse en temps, a fortiori si elle nécessite un déplacement pour être effectuée localement.

2 ANALYSE DES RISQUES ET DEFINITION DES OBJECTIFS DE SECURITE

La prise en compte de la sécurité doit être continue tout au long du projet. Il convient donc de s'appuyer sur une analyse de risque afin de bien définir les critères à prendre en compte. La filière SSI du CIRISI ne disposant pas encore de cette analyse, j'ai donc dû la réaliser.

2.1 METHODOLOGIE

L'une des contraintes de ce projet est que la solution retenue soit proposée en déploiement national. Pour cela elle doit répondre à divers critères relatifs à la sécurité et notamment être homologuée. Ce processus d'homologation nécessite une analyse de risque qui va permettre d'identifier les risques à prendre en compte, les coûts des mesures de sécurité ainsi que les risques assumés. La méthodologie en vigueur au sein du ministère de la défense est « EBIOS » (Expression des Besoins et Identification des Objectifs de Sécurité). C'est donc cette méthode qui a été utilisée afin de réaliser l'analyse.

Pour cadrer avec le projet, l'analyse de sécurité a porté uniquement sur l'activité de télé-administration des EAR. Les autres éléments du système d'information n'ont pas été étudiés afin de limiter le périmètre de l'étude.

Pour cela, l'information nécessaire a été recueillie auprès des clients (utilisateurs : DEX/RZO ainsi que de l'OSSI). Les entretiens ont été réalisés en plusieurs fois afin d'assurer une exhaustivité et une cohérence des réponses obtenues.

2.2 OBJECTIFS DE SECURITE

L'analyse des données récoltées a été faite en s'appuyant sur la base des critères communs. Ceux-ci ont permis d'exprimer les objectifs en besoins de sécurité pour le produit à mettre en œuvre. Ces objectifs sont de trois ordres : Confidentialité, Intégrité et Disponibilité.

Ils constituent l'une des principales composantes de la spécification technique du besoin et feront l'objet d'une validation finale.

L'ensemble des éléments de cette analyse sont disponibles en **annexe A**.

3 RECUEIL DU BESOIN

La problématique du projet est complexe et revêt plusieurs aspects. En effet la solution proposée doit répondre à des objectifs de trois ordres : sécuritaire, organisationnel et économique.

3.1 UN BESOIN DE SECURITE.

Le but principal de la solution doit être de renforcer la sécurité de la fonction télé-administration. L'ensemble des objectifs de sécurité a été défini par l'analyse de risque et traitent tant de la confidentialité que de l'intégrité et de la disponibilité. Ils sont décrit en fin de l'**annexe A**.

3.2 UN BESOIN ORGANISATIONNEL.

Du fait de la réduction de personnels au sein du CIRISI, il est impératif de faire évoluer la fonction de télé-administration. Les outils et procédures actuels ne permettent plus de satisfaire aux contraintes de sécurité en vigueur au sein de l'institution. La politique de changement de mots de passe sur les EAR est excessivement chronophage. De plus, en termes de sécurité il s'avère que de lourdes contraintes de sécurité sont sources de négligence par les utilisateurs.

La fonction de télé-administration devra permettre à un groupe d'utilisateurs restreint (20 personnels) d'appliquer la politique de sécurité interne beaucoup plus rapidement qu'à l'heure actuelle.

3.3 UN BESOIN ECONOMIQUE.

Par ailleurs le fait que la solution implémentée permette une réduction de la charge de travail de ses utilisateurs, induit indirectement des économies. En effet, le volume horaire consacré à l'application de la politique de sécurité s'en trouvera réduit et permettra de dégager des ressources humaines sur d'autres activités.

On constate donc que ces trois aspects sont intrinsèquement liés les uns aux autres. La solution retenue doit donc s'adapter au contexte économique et organisationnel tout en assurant un niveau de sécurité requis.

4 SPECIFICATION DU BESOIN

En l'absence de cahier des charges fourni par le client, j'ai décidé de collaborer avec lui dans la rédaction de celui-ci afin de disposer d'un document final me permettant de recetter le projet.

L'ensemble des exigences et contraintes ont donc été recensées et formalisées. De plus pour chacune, une méthodologie de validation a été convenue avec lui afin de procéder à la recette du produit. L'ensemble a été compilé dans un document nommé « Cahier des charges » disponible en **annexe B**.

4.1 EXIGENCES FONCTIONNELLES

La cible du projet porte sur la fonctionnalité d'authentification sur les EARs. Les objectifs de sécurité fixent la majeure partie des exigences fonctionnelles. Une exigence fonctionnelle supplémentaire a été formulée par le client :

- La TOE doit pouvoir être accessible localement même en cas de défaillance du réseau.

4.2 EXIGENCES NON-FONCTIONNELLES

En ce qui concerne les exigences non-fonctionnelles, elles sont de deux ordres :

Organisationnelles :

- La solution doit permettre de réduire de 66% le temps consacré aux changements des mots de passe.
- La solution doit permettre à un groupe d'utilisateurs restreint (max 20 pax) de mettre en œuvre la PSSI en vigueur.

Technique :

- La solution doit être compatible avec 85% du parc d'équipements actifs minimum.

4.3 CONTRAINTES

Plusieurs contraintes sont également à prendre en compte. Elles sont intrinsèquement liées entre elles notamment de par l'aspect financier et la faible disponibilité des ressources. Elles sont de trois natures :

Organisationnelles :

- Les personnels peuvent avoir une formation interne, mais n'auront pas accès à la formation extérieure pour manager la solution.
  (Il n'y aura pas de budget de formation alloué pour ce projet. Les administrateurs pourront néanmoins recevoir une formation interne pour appréhender le produit.)
- Les ressources en personnel pour le projet sont de 1 personne 3 jours par semaine.
  (Je suis seul à travailler sur le projet tout en conservant mon activité principale en parallèle.)
- La TOE doit respecter la PSSI en vigueur.

Technique :

- La solution doit s'appuyer sur l'Active Directory en place pour authentifier les utilisateurs.
  (L'active Directory existant sera l'annuaire de référence. La solution doit donc s'interfacer avec celui-ci).
- L'ergonomie de l'interface d'administration de la solution doit être une GUI et/ou une WebUI.
  (Hormis les Command Line Interface des équipements actifs, les utilisateurs ne souhaitent pas de CLI. Une interface graphique pour l'administration de la solution d'authentification est préférable).
- La solution doit s'intégrer dans l'architecture actuelle. (SHEM / virtualisation).
  (L'architecture actuelle est basée sur de la virtualisation. La solution doit donc pouvoir être virtualisée).
- La solution ne doit pas modifier la configuration des postes client d'administration.
  (Aucune installation de client lourd ne doit être faite. Seul un client SSH déjà existant doit être présent sur les postes).

Financières :

- La solution ne doit pas engendrer de coûts supplémentaires à ceux déjà engagés.
  (Aucun budget n'a été alloué pour ce projet. La solution s'appuiera sur les ressources existantes et disponibles).

III CONCEPTION

Lors de cette étape, un état de l'art va être fait. Celui-ci permettra, d'une part, de comparer les solutions existantes et d'autre part, de pouvoir sélectionner les composants du produit qui répondent le mieux au cahier des charges. L'architecture globale de la solution va ainsi être définie.

1 PRISE EN COMPTE DE L'EXISTANT ET CONCEPTION DE L'ARCHITECTURE

L'analyse des contraintes et des fonctionnalités souhaitées ainsi que la prise en compte de l'existant permettra de définir les composants de la solution à mettre en place. Par ailleurs, la solution devra préciser les mesures qui permettront de répondre distinctement aux 75 points du cahier des charges. L'architecture globale sera définie en fonction de tous ces éléments.

L'une des contraintes précise que l'authentification doit s'appuyer sur l'annuaire Active Directory. Cela implique que les EAR puissent s'interfacer avec l'annuaire Active Directory. Il faut donc inclure à la solution un serveur d'authentification s'appuyant sur l'Active Directory.

Par ailleurs, les différents protocoles de communications liés au processus d'authentification doivent eux aussi être sécurisés.

Ensuite, les exigences fonctionnelles liées à la traçabilité impliquent un élément de journalisation.

Enfin, les postes d'administration ainsi que les EAR font partis des éléments déjà existants devant être pris en compte.

La solution va donc s'apparenter au schéma de la figure 8 ci-dessous :

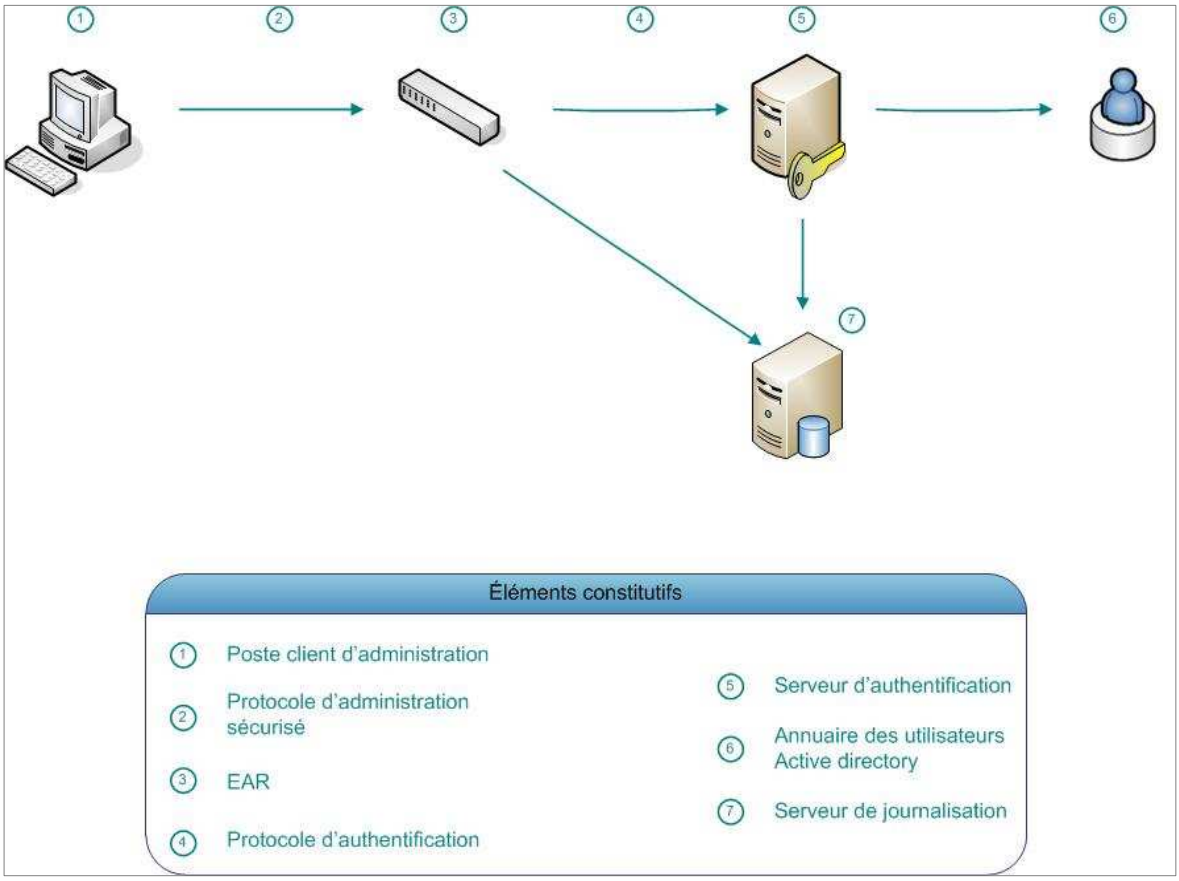


Figure 8 : Éléments de constitutifs de la solution

Certains **éléments sont existants et devront être pris en compte** dans la solution proposée. Ils ne pourront donc pas faire l'objet d'une bascule au profit d'un produit analogue. Ces éléments sont :

- les postes clients d'administration,
- les EARs
- l'annuaire des utilisateurs AD.

Les autres **éléments devront faire l'objet d'un comparatif** avant d'arrêter leur choix. Il convient donc d'effectuer un état de l'art concernant :

- les solutions de télé-administration.
- Les solutions d'authentification (protocole et serveur).
- Le serveur de journalisation.

2 ÉTAT DE L'ART ET VALIDATION DES COMPOSANTS

Cette étape du projet consiste à sélectionner les produits qui répondent le mieux aux critères de choix.

Les critères qui ont influé fortement sur la sélection des produits sont :

- Le niveau de sécurité,
- L'ergonomie,
- La compatibilité avec l'ensemble de la solution,
- Le coût,
- L'adéquation aux besoins quantitatifs du projet,
- Le support disponible.

Dans les paragraphes suivants, ces critères sont mis en relief dans les comparatifs des différents éléments au travers de la signalétique suivante :

Avantage substantiel

Inconvénient rédhibitoire

2.1 LES SOLUTIONS DE TELE-ADMINISTRATION.

Il existe plusieurs méthodes de télé-administration ayant chacune leurs avantages et leurs inconvénients tant vis-à-vis de l'ergonomie, de la confidentialité que de implémentation. Les principaux critères d'évaluation retenus sont la sécurité, l'ergonomie et la normalisation de la solution.

	Avantages	**Inconvénients**
SNMP	+ protocole standardisé + Permet la configuration simplifiées des EAR via les MIB + Implémenté sur l'ensemble des EAR	- Protocole non-sécurisé avant la version 3 - N'authentifie pas individuellement les utilisateurs (principe de communauté) - Tous les équipements actifs n'implémentent pas la V3 - Certaines MIB ne sont pas disponibles (limitation des fonctionnalités d'administration)
Telnet	+ protocole standardisé + Permet l'utilisation d'un Shell + Implémenté sur l'ensemble des EARs	- protocole non-sécurisé
SSH	+ protocole standardisé + Permet l'utilisation d'un Shell + Implémenté sur l'ensemble des EARs récents + Protocole sécurisé + protocole déjà utilisé par le client	- Paramétrage légèrement plus complexe que celui de Telnet (sécurité)
WebUI	+ ergonomie plus conviviale	- Absolument pas standardisé - Interfaces souvent sources de vulnérabilités - Commandes fortement limitées

Figure 9 : Comparatif des solutions de télé-administration

Comme le présente la figure 9 et compte tenu de la nécessité de sécuriser les connexions entre la station d'administration et l'EAR, le protocole SSH a été retenu. C'est le protocole de télé-administration le plus sécurisé étudié et il nécessite simplement un client (portable apps) sur la station d'administration qui n'en modifie pas la configuration et ne nécessite aucune installation. Par ailleurs, l'ensemble du parc d'EAR est compatible avec ce protocole. Enfin, les administrateurs l'utilisent déjà et sont donc habitués à son exploitation.

2.2LES PROTOCOLES D'AUTHENTIFICATION

L'analyse de risque fait apparaître que plusieurs fonctions doivent impérativement être implémentées. En l'occurrence : l'authentification, l'autorisation, la traçabilité.

On parle alors d'architecture AAA (Authentication, Authorization and Accounting).

L'analyse des protocoles va se focaliser sur ceux implémentant ces fonctionnalités. On peut retenir trois protocoles principaux présentés à la figure 10 : RADIUS, DIAMETER, TACACS+.

	Avantages	**Inconvénients**
RADIUS	+ Protocole standardisé + Implémenté sur la majorité des EAR (>85%) + Protocole largement répandu avec un fort retour d'expérience	- N'a pas la fiabilité de communication de TCP
DIAMETER	+ protocole standardisé + Protocole en mode connecté (TCP) + Successeur de RADIUS	- Encore peu implémenté sur l'ensemble des EAR
TACAS+	+ Protocole en mode connecté (TCP) + Peut utiliser le transport réseau sécurisé (Ipsec TLS) + Authentification et autorisation indépendant	- Protocole Propriétaire CISCO. Non implémenté sur les matériels autres que CISCO.

Figure 10 : Comparatif des protocoles d'authentification

Pour ce qui est des protocoles d'authentification, TACACS+ est une solution propriétaire de CISCO et n'est pas implémentée sur l'ensemble du parc d'EAR.

DIAMETER est une solution récente qui offre des avantages techniques certains mais peu d'équipements cibles sont compatibles.

Le protocole RADIUS offre un niveau de sécurité satisfaisant et il est possible de l'implémenter sur la majeure partie du parc d'EAR ce qui répond à la contrainte de compatibilité sur 85% minimum des équipements. C'est donc le choix du protocole Radius qui a été retenu. Il sera mis en œuvre via le produit Microsoft NPS (Network Policy Services) car ce dernier s'intègre parfaitement à l'architecture Microsoft en place et les licences sont déjà disponibles pour ce produit dans le cadre d'un marché national.

2.3 LES SERVEURS DE JOURNALISATION.

Il convient de bien décomposer les fonctions du serveur de journalisation. Il doit d'une part centraliser les journaux d'événement et d'autre part les stocker et offrir une interface de gestion de ces derniers.

Ces points vont donc être analysés distinctement.

2.3.1 LA CENTRALISATION DES JOURNAUX D'EVENEMENT

Deux formats principaux de journalisation coexistent : Syslog pour les EAR et les serveurs UNIX / LINUX et Eventlog pour les serveurs Microsoft. Cependant, ce dernier format étant propriétaire de Microsoft, la majorité des équipements actifs sont uniquement compatibles avec le format Syslog. L'importance du nombre d'EAR implique d'implémenter une solution compatible avec l'ensemble du parc.

Une multitude de produits existent sur le marché. Cependant il convient d'étudier leurs coûts, leurs méthodes de stockage des journaux, leur compatibilité ainsi que leur fonctionnalités particulières. La figure 11 compare de manière non exhaustive un panel de solutions de recueil de journaux.

	Avantages	**Inconvénients**
Syslog-ng	+ Solution mature. Ayant évoluée depuis son apparition en 1998 + Stockage des journaux en BDD possible + Grande compatibilité + Grande communauté	- Toutes les options ne sont pas disponibles dans la version communautaire - Limitation à environ 75 000 logs / jours /serveur
Rsyslog	+ Stockage des journaux en BDD possible + Grande compatibilité + Grande communauté + Basé sur syslog-ng + Ajoute des modules réservés à la version payante de syslog-ng + Client Windows disponible et modulable	- Nécessite une configuration précise pour traiter les journaux « eventlogs »
ArcSight	+ Solution clef en main + Intègre une interface de gestion	- Appliance - Payant - Versions limités en taille, en nombre de client et de journaux par seconde.

Winsyslog	+ Produit mature (existe et évolue depuis 1996) + Grand nombre d'options de configuration + Intègre une interface de gestion	- Payant - Versions limités en nombre de client et de journaux par seconde.
SNARE	+ Intègre une interface de gestion + Grand nombre d'options de configuration	- Agent open source mais serveur payant - Appliance
GFI event Manager	+ Intègre une interface de gestion + Solution très complète + Acteur majeur du domaine	- Payant

Figure 11 : Comparatif des serveurs de centralisation des journaux d'événements

1.1.1 LA GESTION DES JOURNAUX D'EVENEMENT

Pour ce qui concerne les solutions de gestion, il convient de bien prendre en compte l'ergonomie du produit. En effet, les utilisateurs devront pouvoir utiliser facilement la solution retenue. De plus, elle doit être dimensionnée à hauteur du parc d'éléments à administrer.

Le tableau de la figure 12 compare différents produits répondant tout ou partie aux besoins exprimés.

	Avantages	**Inconvénients**
PHP-Syslog-ng	+ Solution largement documentée + Interface WEB + Produit initialement gratuit	- Produit payant depuis la version LOGZILLA, donc support payant.
WallWatcher	+ Stockage des journaux en BDD possible	- Shareware
ArcSight	+ Solution clef en main	- Appliance

Winsyslog	+ Produit mature (existe et évolue depuis 1996)	- Payant
SNARE	+ Intègre une interface de gestion+	- Agent open source mais serveur payant - Appliance
GFI event Manager	+ Intègre une interface de gestion + Solution très complète + Acteur majeur du domaine	- Payant
Loganalyzer	+ Solution gratuite + Interface compatible eventlog et Syslog + Possibilité de configuration importante + S'adapte à plusieurs formats de stockage + Grande communauté + Web UI	- Nécessite de bien configurer le produit

Figure 12 : comparatif des solutions de gestion des journaux d'événements

Pour le serveur de journalisation, la puissance du logiciel RSYSLOG, sa gratuité ainsi que la communauté disponible autour de ce produit en font le choix le plus pertinent. Il est suffisamment mature pour les besoins de la solution et présente l'avantage d'être directement implémenté sur un grand nombre de distributions.

En ce qui concerne la gestion des journaux d'événement, le choix s'est porté sur le logiciel gratuit « LOGANALYZER ». En effet, il offre la possibilité d'exploiter des fichiers comme des bases de données. Il fournit une interface simple et configurable. Par ailleurs, il permet d'analyser autant les journaux « EVENTLOG » que ceux au format « SYSLOG ». Il convient donc très bien aux besoins du projet.

La contrainte légale de stockage des journaux d'événement d'une durée d'un an nécessite beaucoup de place. Le stockage des données dans des fichiers « à plat » n'est pas envisageable car l'exploitation de ceux-ci serait trop fastidieuse. Une base de données sera donc utilisée. Le schéma de celle-ci sera définit par l'interface de gestion.

3 ARCHITECTURE RETENUE

L'ensemble de la solution sera donc composée tel que le décrit la figure 13 ci-dessous :

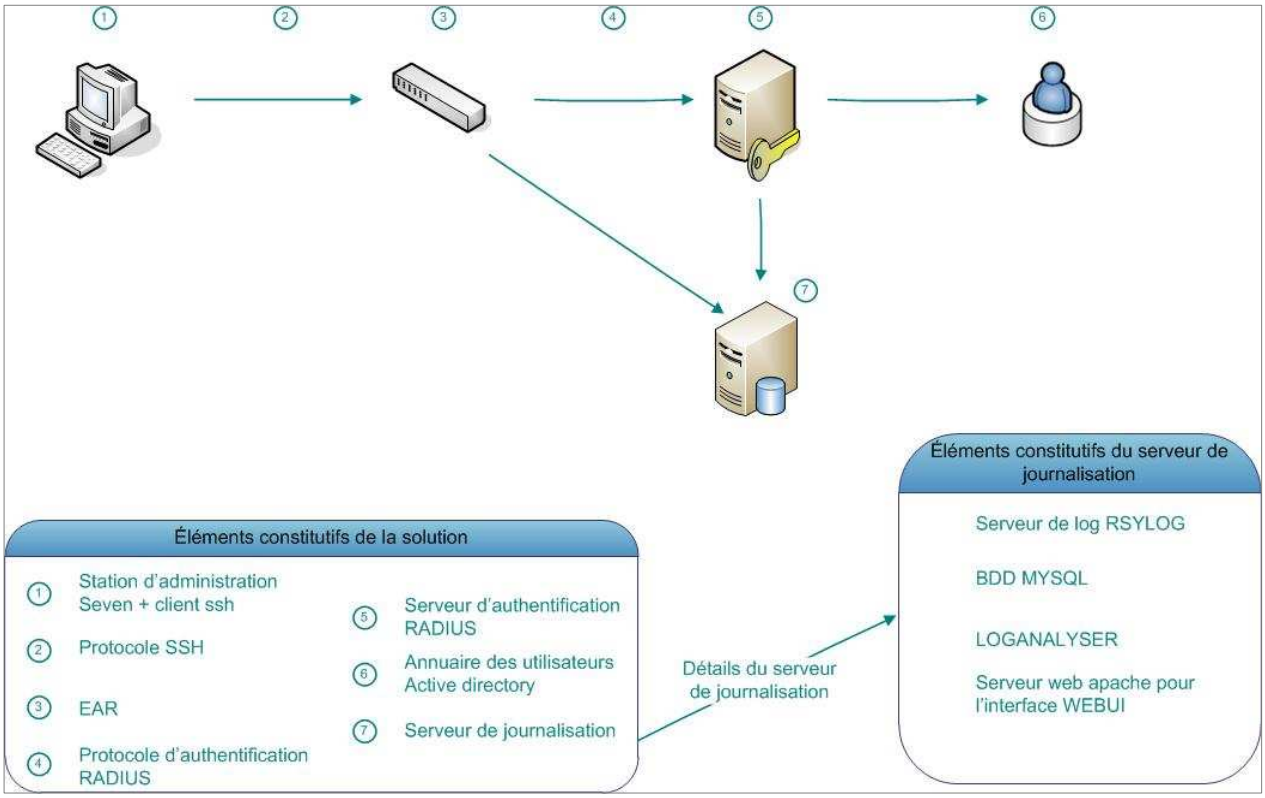


Figure 13 : maquette de la solution à réaliser.

En ce qui concerne le processus d'authentification, il procédera comme le décrit la figure 14 :

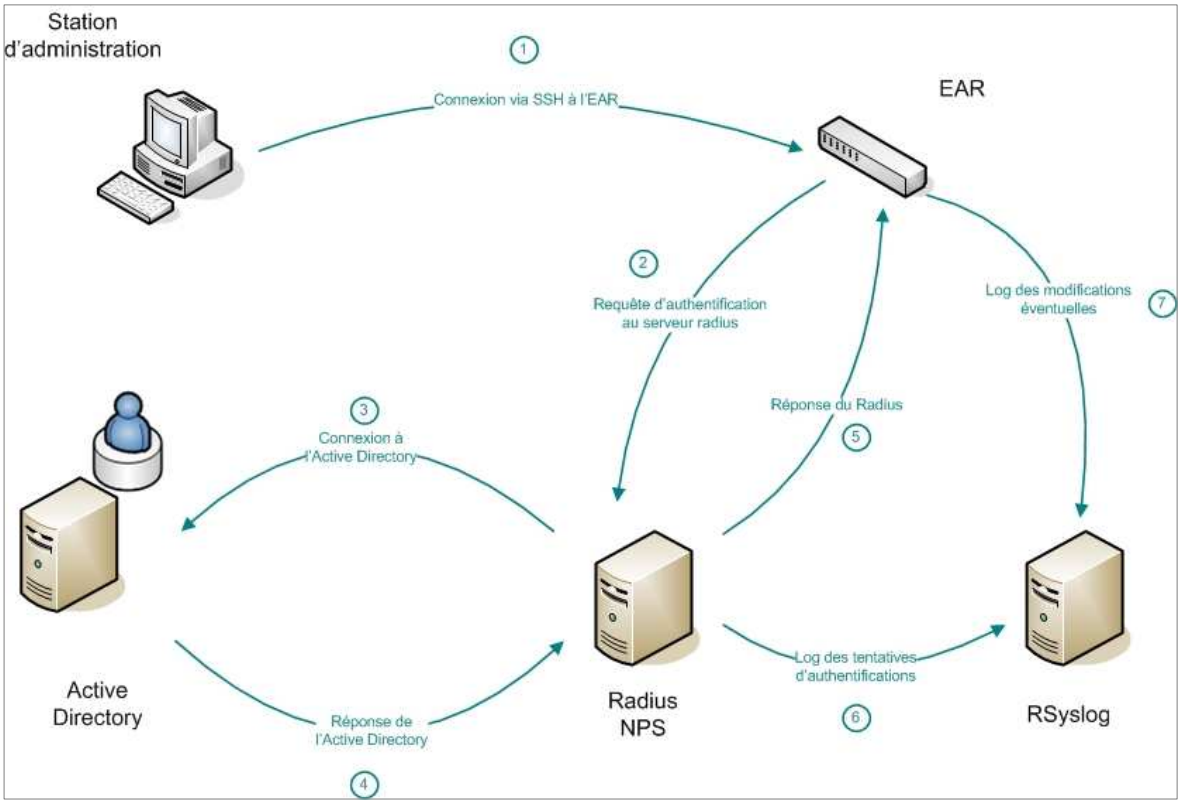


Figure 14 : Processus d'administration d'un EAR

4 COORELATION DE LA SOLUTION AVEC LE BESOIN

L'ensemble des éléments exprimés et recensés lors de la phase de spécification du besoin ont donc été collationnés dans le « cahier des charges » (**annexe B**). Une fois la solution conçue, chacun de ces points est solutionné par la mise en place d'une ou plusieurs mesures ainsi qu'une méthode de recette. Quand ces mesures sont d'ordre technique, les éléments de l'architecture impliqués sont spécifiés. Ainsi les 75 points sont mis en relation avec les éléments du projet.

Ex :

Point N°	**Détail du besoin**	**Mesure mise en place**
16	**Imputabilité** = données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de la tentative d'accès ; réussite de la tentative.	RSYSLOG

IV REALISATION

L'architecture mise en place comporte trois éléments centraux :

- L'authentification
- La traçabilité
- L'autorisation

C'est ce qui s'appelle une architecture AAA (Authentication, Authorization, Accounting = Authentification, Autorisation, Traçabilité).

La phase de réalisation va donc consister à organiser l'activité afin d'implémenter ces trois fonctions.

1 ORGANISATION DE LA PHASE DE REALISATION

Le contexte, la disponibilité des ressources ainsi que l'environnement de production induisent des contraintes nécessitant une adaptation de la phase de réalisation.

Ces éléments sont expliqués ci-après.

1.1 RESSOURCES EXPERIMENTALES

La virtualisation offre de nombreux avantages pour la réalisation d'une plateforme de test. En effet, il est aisé de sauvegarder un environnement de configuration, le modifier et éventuellement y revenir. De plus, l'indépendance avec l'environnement de production permet de s'affranchir temporairement de nombreuses contraintes. Ainsi, il est alors possible de simplifier l'architecture et l'étendue des droits d'administration est accrue.

Par ailleurs, le fait de travailler en environnement virtualisé, limite les problèmes de sécurité. En effet, aucun élément ne peut interagir avec l'environnement de production et vice versa.

Du fait de la disponibilité d'une baie de virtualisation (ESXi5), j'ai décidé de procéder à la réalisation des tests en environnement virtualisé même si il m'est impossible de prendre en compte l'ensemble des contraintes environnementales.

1.2 CONTRAINTES ENVIRONNEMENTALES

Comme cela a été précisé en introduction, le CIRISI est issu du regroupement des services informatiques de plusieurs entités de sa zone de responsabilité. Ainsi, avant 2010, chaque service gérait de manière indépendante son système d'information. Tout en respectant un cadre de préconisations nationales (notamment relatives à la sécurité), chaque entité appliquait ses propres procédures, équipait son parc avec le matériel qu'elle jugeait opportun et architecturait son système d'information librement.

Le parc est en constante évolution et certains matériels sont en cours de renouvellement. Ainsi certains équipements vieillissants vont être renouvelés au profit de matériels plus récents.

Cependant, le parc d'équipements actifs réseau est actuellement très hétérogène. Lors du recensement effectué au début du projet, il existait 42 modèles différents d'équipement fournis par 7 constructeurs. L'implémentation du protocole RADIUS étant laissée partiellement à la discrétion des fournisseurs, cette variété d'équipement induit une forte complexité.

Par ailleurs, il n'est pas possible de mettre à disposition les 42 modèles différents d'équipements pour la phase de réalisation du projet. S'il est aisé de virtualiser du matériel CISCO, il n'en est pas de même pour ceux d'autres fournisseurs.

Ce point précis a donc conditionné la planification de la phase de réalisation.

1.3 PLANIFICATION

Du fait de l'impossibilité de virtualiser toute la diversité d'équipement actif réseau, j'ai décidé de procéder en deux étapes majeures.

La première étape aura pour but de réaliser un prototype d'architecture en environnement virtualisé. Celui-ci permettra notamment de configurer et de faire valider par le client les interfaces ainsi que les fonctionnalités d'authentification et de traçabilité. Ces deux fonctions étant très peu dépendantes des EAR, un seul matériel constructeur sera virtualisé (matériel CISCO) et suffira à faire valider cette partie du projet par le client.

L'authentification et la gestion des autorisations sont extrêmement liées dans ce projet. Le prototype implémentera donc une fonctionnalité de gestion des autorisations mais son périmètre sera uniquement réduit aux matériels virtualisés.

Ensuite, une fois le prototype validé, une version de pré-production sera mise en place. Celle-ci sera intégrée à l'environnement de production sans toutefois en être une composante. Cette étape aura pour finalité de procéder au paramétrage de la fonctionnalité d'autorisation sur l'ensemble du parc d'EAR. En effet, comme il a été précisé supra, cette gestion est fortement liée aux spécificités du constructeur.

C'est cette version qui sera recettée, puis déployée et mise en production.

Comme cela est représenté sur la figure 15, la réalisation va donc se faire selon ces deux étapes : « Prototypage » et « pré-production ».

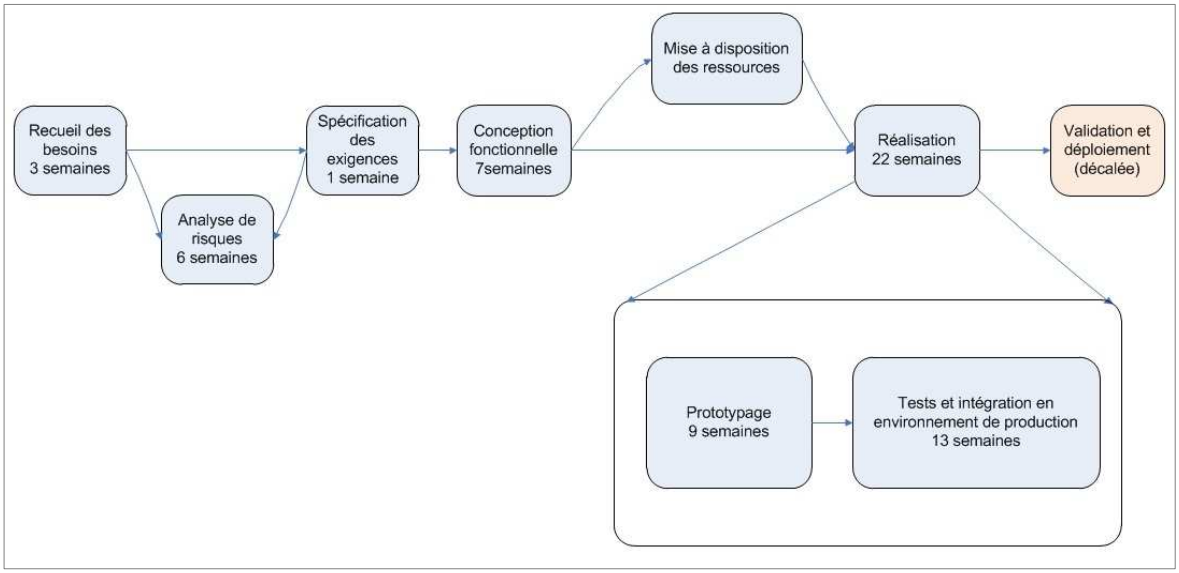


Figure 15 : planification générale du projet

2 LE PROTOTYPE

Le prototype de la solution a donc plusieurs objectifs. Entre autres, il vise à :

- architecturer les composants retenus,
- faire valider l'ergonomie de la solution,
- implémenter les fonctionnalités d'authentification et de traçabilité.

Rappelons que la fonctionnalité d'autorisation fera pour sa part l'objet de la phase de pré-production.

Par ailleurs, si besoins est, le prototype permet de gérer précocement les modifications afin d'éviter toute mauvaise surprise lors de la recette finale.

Le prototype est tout d'abord décomposé en tâches nécessaires à sa réalisation. Celles-ci sont ensuite décomposées en lots qui sont priorisés en fonction de leur interdépendance et de la valeur de risque qui leur est attribué. Ce risque est directement lié à la complexité de chaque lot ainsi que de son interdépendance avec les autres lots.

Le traitement des lots est fait de manière itérative jusqu'à validation. Ainsi, en cas de problème technique, l'ensemble de la solution n'est pas entièrement remis en cause.

Cette conduite de projet permet d'éviter un effet « tunnel » pour le client, qui l'exclurait de la phase de réalisation.

2.1 ARCHITECTURE DU PROTOTYPE

Le prototype n'étant pas directement lié à l'environnement de production, il est possible d'en réduire sa complexité en mettant en place une architecture « épurée ». À cet effet, et compte tenu de mon expérience dans le domaine de la virtualisation, j'ai pris la décision de réaliser l'ensemble des tests dans un environnement virtuel comme initialement prévu.

La plate-forme de virtualisation disponible est un hyperviseur ESXI5. Ce produit permet nativement de virtualiser des systèmes d'exploitation et des réseaux mais pas les firmwares CISCO (IOS). Il est cependant possible d'utiliser le logiciel GNS3 qui offre cette fonctionnalité. Celui-ci peut fonctionner dans un environnement Microsoft ou Linux.

Il existe une distribution Linux dédiée à la virtualisation de firmwares CISCO nommée « HOT4 ». Cette distribution est soutenue par des personnels du cours réseau de l'école des transmissions de l'armée de terre (ETRS). Pour rappel, l'ETRS est un client du CIRISI Rennes. La plus-value en termes de support n'étant pas négligeable, c'est donc cette distribution que j'ai retenue pour virtualiser les équipements.

L'architecture du prototype sera conforme à celle présentée par la figure 16 ci-dessous :

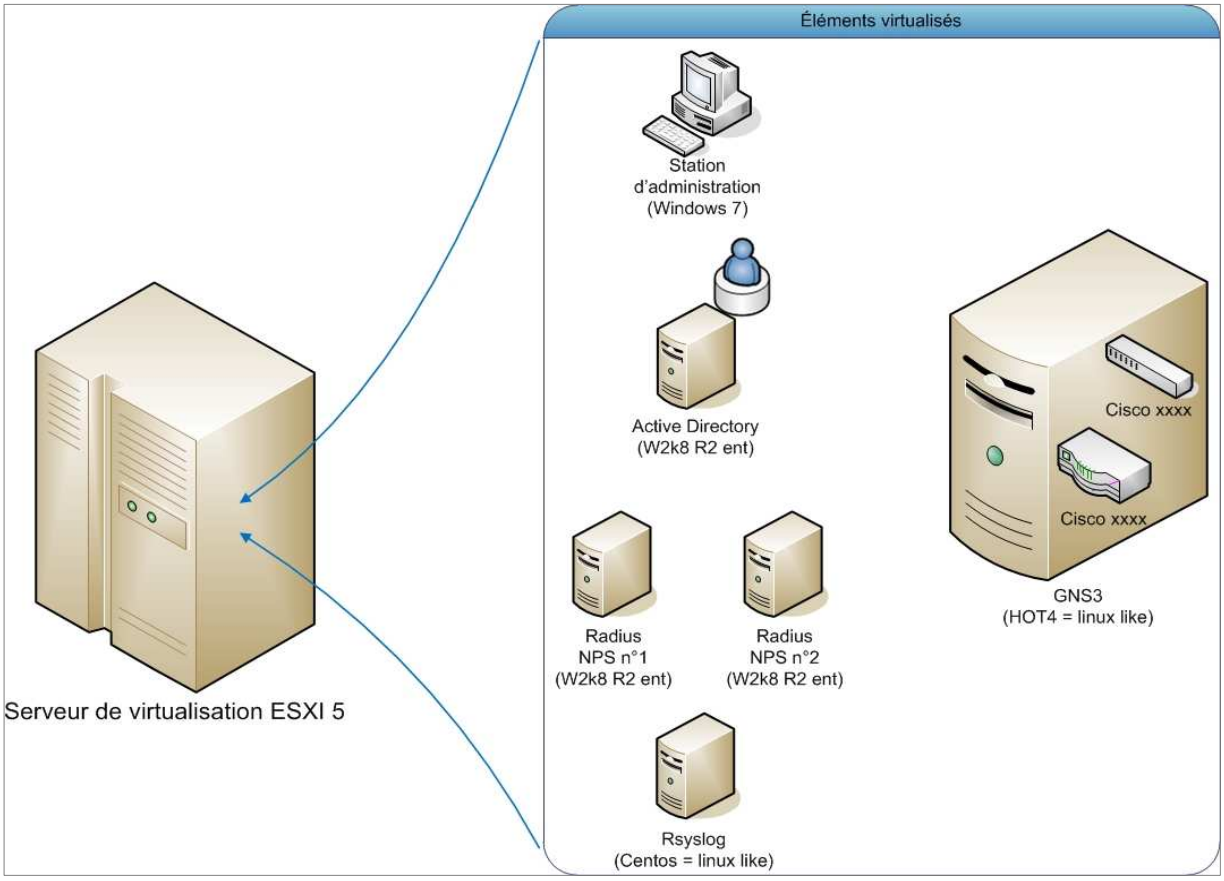


Figure 16 : architecture du prototype

2.2 GESTION DE PROJET

2.2.1 DECOMPOSITION ET PLANIFICATION DES TACHES

Le prototype à mettre en œuvre a été décomposé en plusieurs éléments distincts appelés « LOT ». Ces éléments ont ensuite été organisés en fonction de leur interdépendance comme le montre la figure 17 ci-dessous :

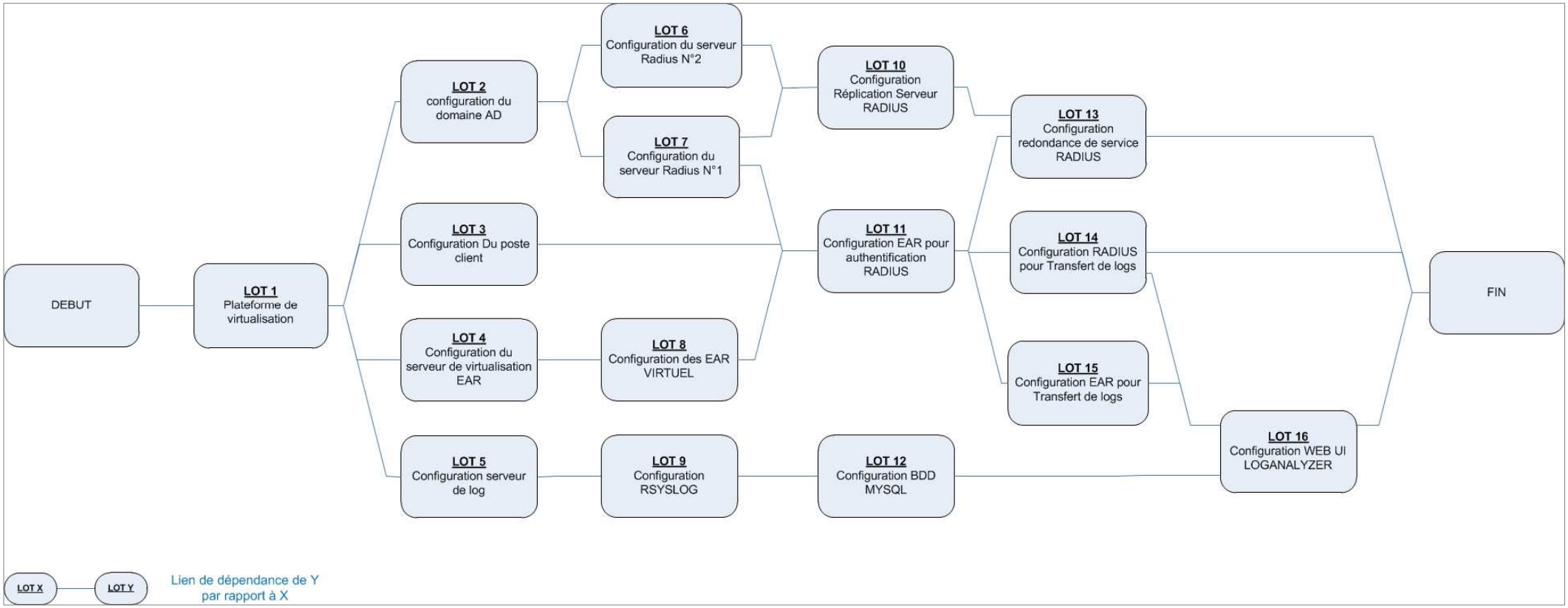


Figure 17 : Interdépendance des lots du prototype

Certains lots ont pu être réalisés en parallèle. Cependant, une notion de risque a été introduite afin de prioriser au maximum la réalisation des lots. J'ai défini ce risque en fonction de mon expérience sur les technologies à déployer ainsi que sur l'interdépendance des lots sur les uns par rapport aux autres.

Le tableau de la figure 18 ci-après présente l'évaluation des risques des divers lots.

Descriptif de la Tâche	Numéro de lot	Priorité	Risque
Plateforme de virtualisation	LOT 1	1	1
Configuration du domaine Active Directory	LOT 2	2	1
Configuration du poste client	LOT 3	2	1
Configuration du serveur de virtualisation EAR (HOT4)	LOT 4	2	3
Configuration OS CENTOS du serveur de log	LOT 5	2	1
Configuration du serveur RADIUS N°2	LOT 6	3	1
Configuration du serveur RADIUS N°1	LOT 7	3	3
Configuration des EAR virtuels	LOT 8	3	2
Configuration RSYSLOG	LOT 9	3	4
Configuration réplication serveur RADIUS	LOT 10	4	2
Configuration EAR pour authentification RADIUS	LOT 11	4	2
Configuration BDD MySQL	LOT 12	4	2
Configuration redondance du service RADIUS	LOT 13	5	3
Configuration RADIUS Pour Transfert de logs	LOT 14	5	2
Configuration EAR Pour Transfert de logs	LOT 15	5	2
Configuration WebUI LOGANALYZER	LOT 16	6	3

Figure 18 : évaluation des risques des lots du prototype.

La planification du développement des composants a donc été organisée en fonction des dépendances des lots ainsi que l'évaluation des risques associés. Il en résulte la planification de la figure 19 :

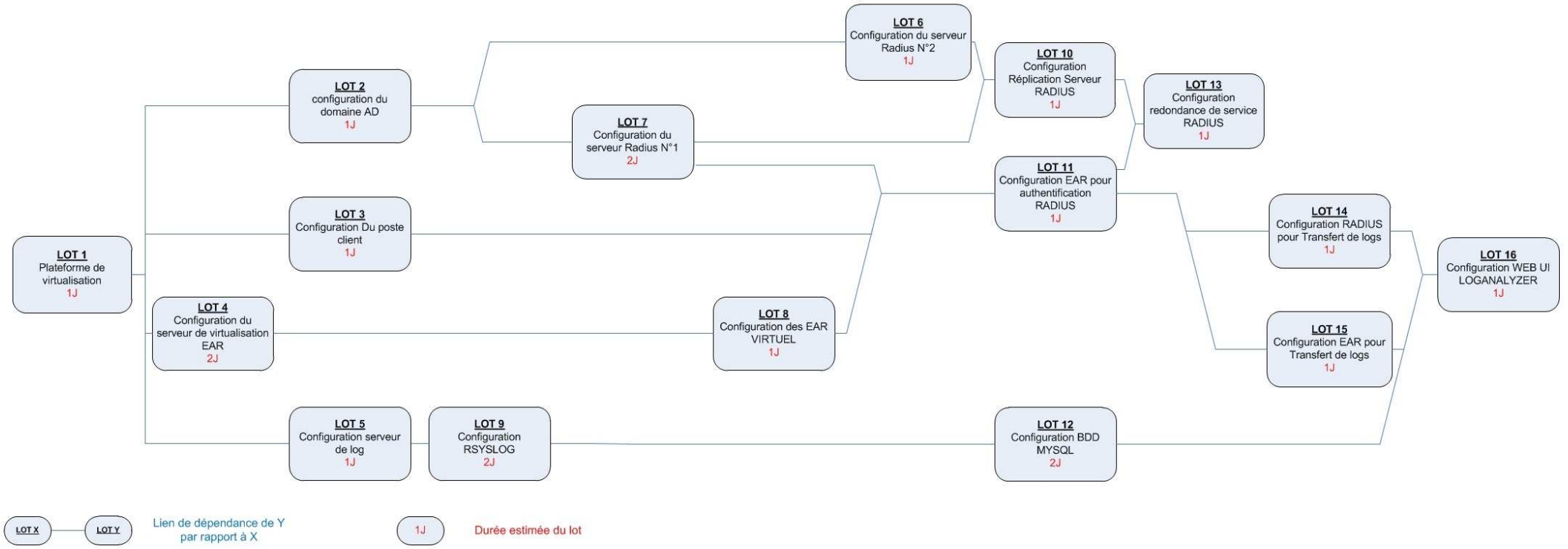


Figure 19 : Planification du développement des composants du prototype

2.2.2 DEVELOPPEMENT ET CONFIGURATION DES COMPOSANTS

Comme précisé auparavant chaque composant a été développé suivant un processus itératif. En effet, chaque élément suit un cycle plus ou moins long qui permet au client de suivre l'évolution du développement du produit. Ce cycle est celui présenté par la figure 20 ci-après :

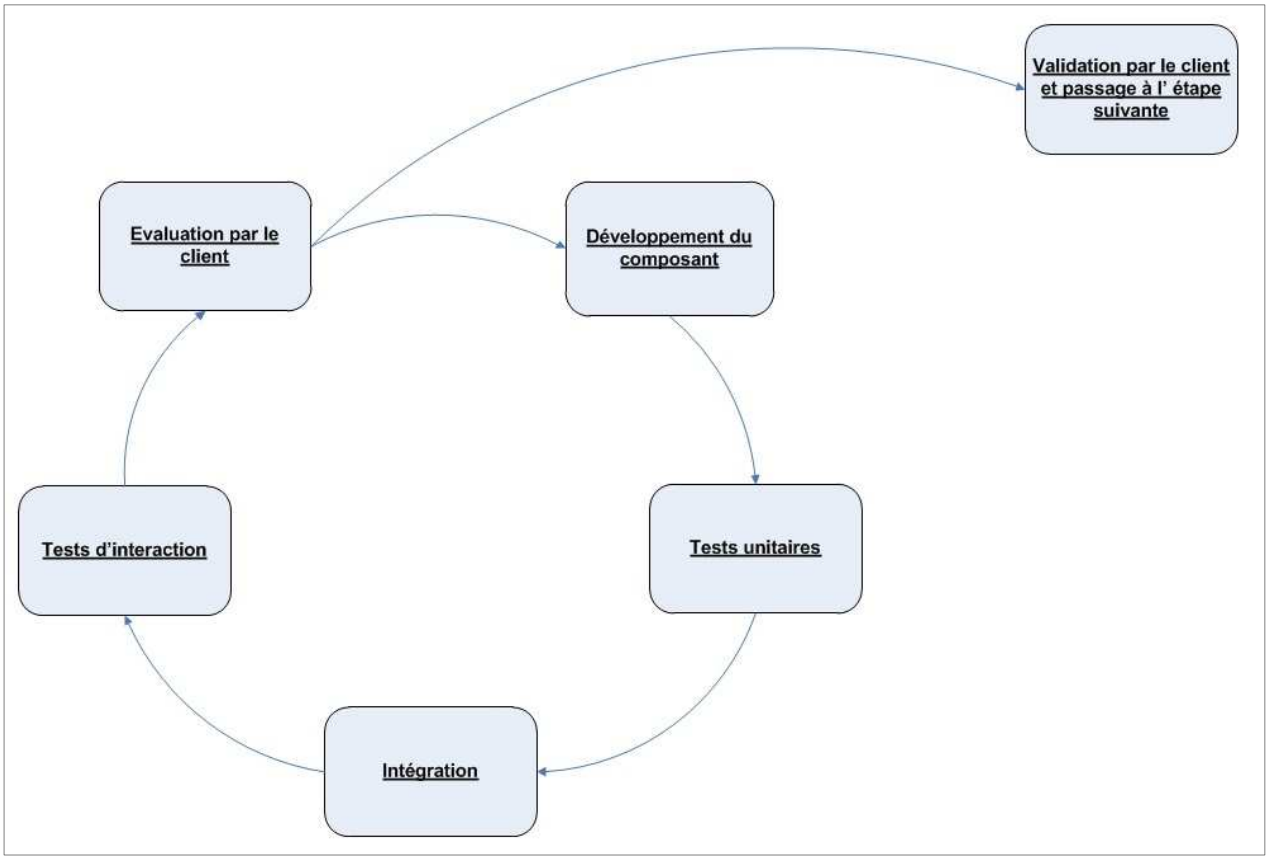


Figure 20 : cycle des itérations

2.3IMPLEMENTATION DE L'AUTHENTIFICATION

Historiquement, l'authentification sur les EAR se faisait avec une base de comptes locaux aux équipements. Le projet a été conçu pour que la fonctionnalité d'authentification se base sur l'annuaire des comptes de l'Active Directory déjà existant au sein du système d'information.

Si nativement l'Active Directory implémente l'authentification Kerberos, ce n'est pas le cas des équipements cibles. Il a donc fallu que les EAR puissent s'interfacer avec cet annuaire et c'est pour cette raison que le choix du protocole RADIUS a été fait lors de la phase de conception.

La figure 21, ci-dessous, représente les échanges protocolaires permettant l'administration des EAR. Ce sont plus précisément les étapes 1 à 5 qui sont impliquées dans le processus d'authentification.

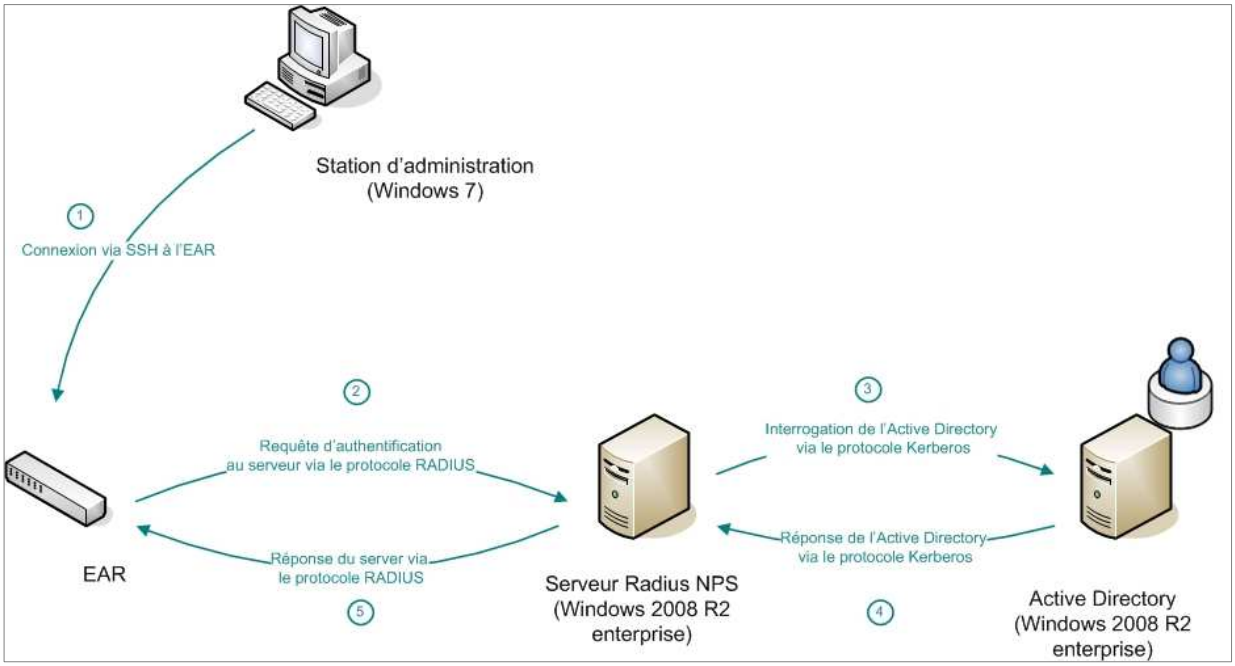


Figure 21 : Processus d'administration d'un EAR

1. Lors de l'étape 1, le client établit une connexion à l'EAR cible en s'appuyant sur le protocole SSH dédié à cette tâche.

2. Ensuite, dans la configuration du projet, l'équipement ne consulte plus une base de comptes locaux, mais établit une communication avec le serveur RADIUS en s'appuyant sur le protocole RADIUS.

3. Le serveur RADIUS interroge l'Active Directory via le protocole KERBEROS.

4. Le contrôleur de domaine Active Directory traite la requête d'authentification du serveur RADIUS et renvoie une réponse (favorable ou pas).

5. Le serveur RADIUS transfert un message à l'équipement soit de validation des informations d'identification, soit d'invalidation.

2.3.1 CONFIGURATION DES EARS

La configuration des EAR est relativement simple. Quasiment tous les modèles récents sont compatibles avec l'authentification RADIUS. Pour effectuer le paramétrage des fonctionnalités AAA, il existe un menu de configuration adapté.

Dans le cas du prototype, la configuration s'est donc faite sur du matériel CISCO. Pour un routeur CISCO 3745 (IOS version 12.4), le nom du menu de configuration AAA est éponyme : AAA.

La configuration de l'EAR se déroule tel que décrit ci-dessous (cf. figure 22) :

1. Créer un nouveau modèle AAA. Il sera le cadre général du paramétrage des fonctionnalités AAA de l'EAR.

2. Définir les serveurs RADIUS. Chaque serveur RADIUS est déclaré ainsi que les ports de communication utilisés s'ils ne sont pas standards. Une clef secrète est paramétrée pour chiffrer les échanges avec les serveurs.

3. Définir un groupe de serveur radius. Celui-ci regroupera l'ensemble des serveurs RADIUS.

4. Déclarer un mode d'authentification AAA s'appuyant sur le groupe radius créé.

5. Paramétrer l'ouverture de session sur les consoles virtuelles. Ces dernières doivent accepter uniquement le protocole SSH, s'appuyer sur l'authentification RADIUS et s'appuyer sur la gestion des autorisations RADIUS.

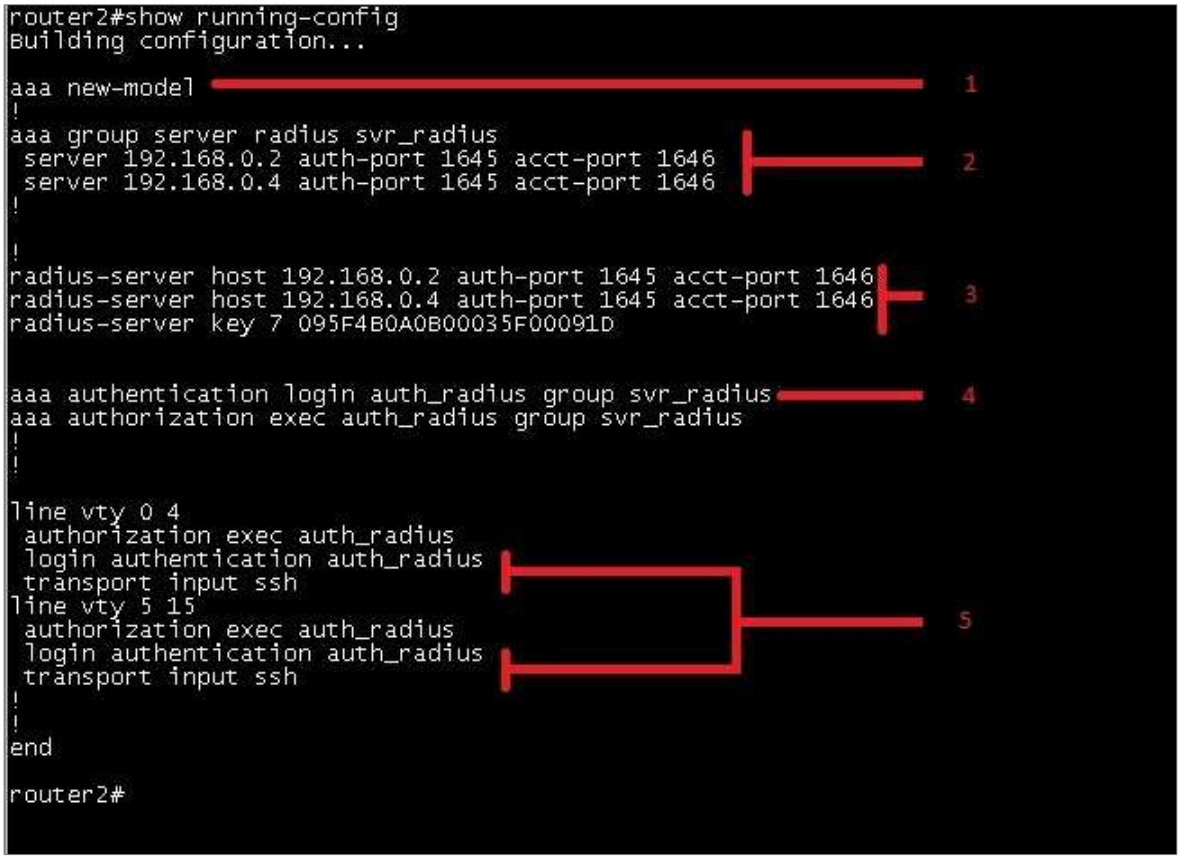


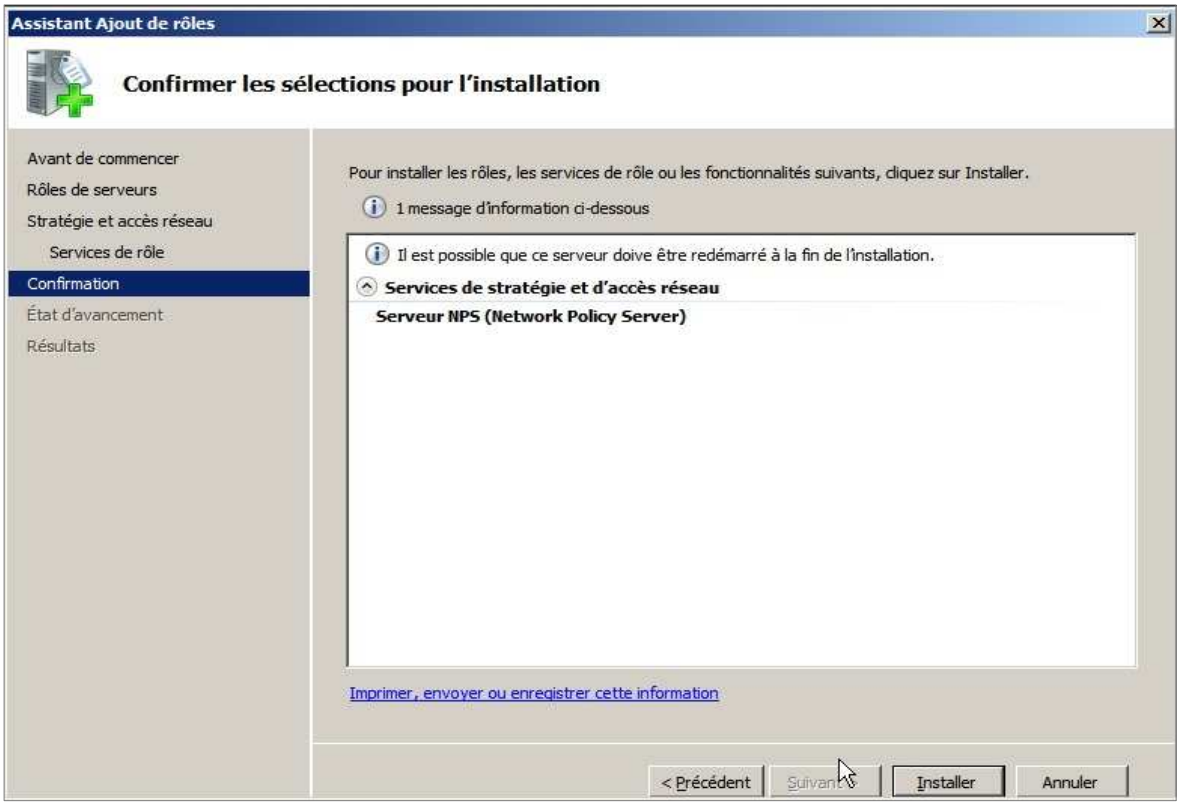
Figure 22 : Configuration authentification RADIUS sur un EAR CISCO

2.3.2 CONFIGURATION DES SERVEURS NPS

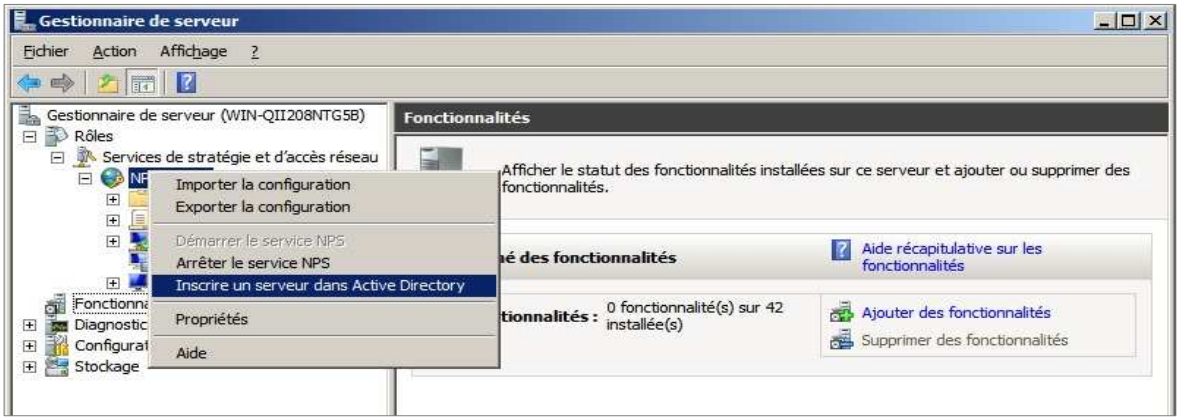
Le serveur Microsoft RADIUS NPS (Network Policy Server) s'interface parfaitement avec l'Active Directory. De plus, son ergonomie correspond aux exigences du client.

La configuration du serveur NPS comporte 5 étapes principales :

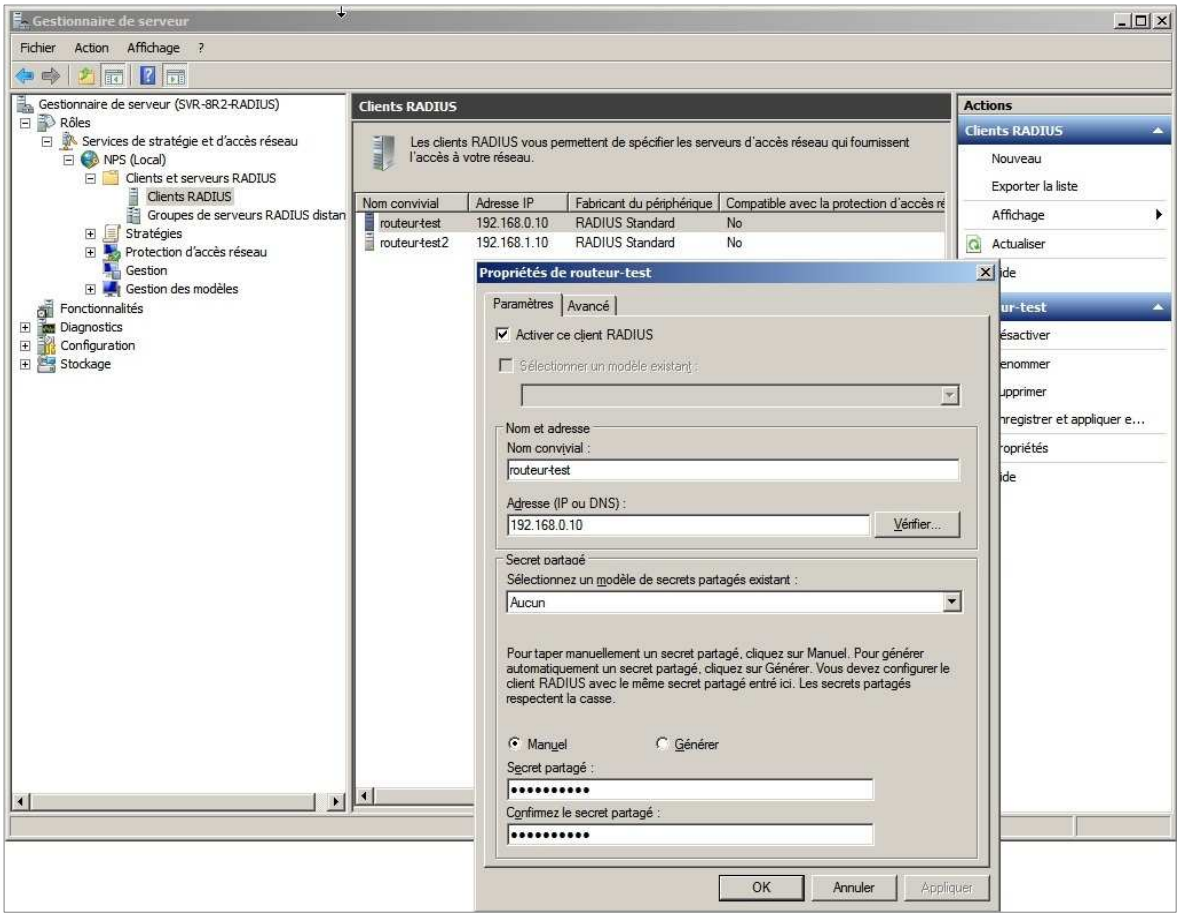
1. En premier lieu, il faut ajouter le « rôle de Services de stratégie et d'accès réseau » au serveur Microsoft Windows Server 2008 R2 entreprise.



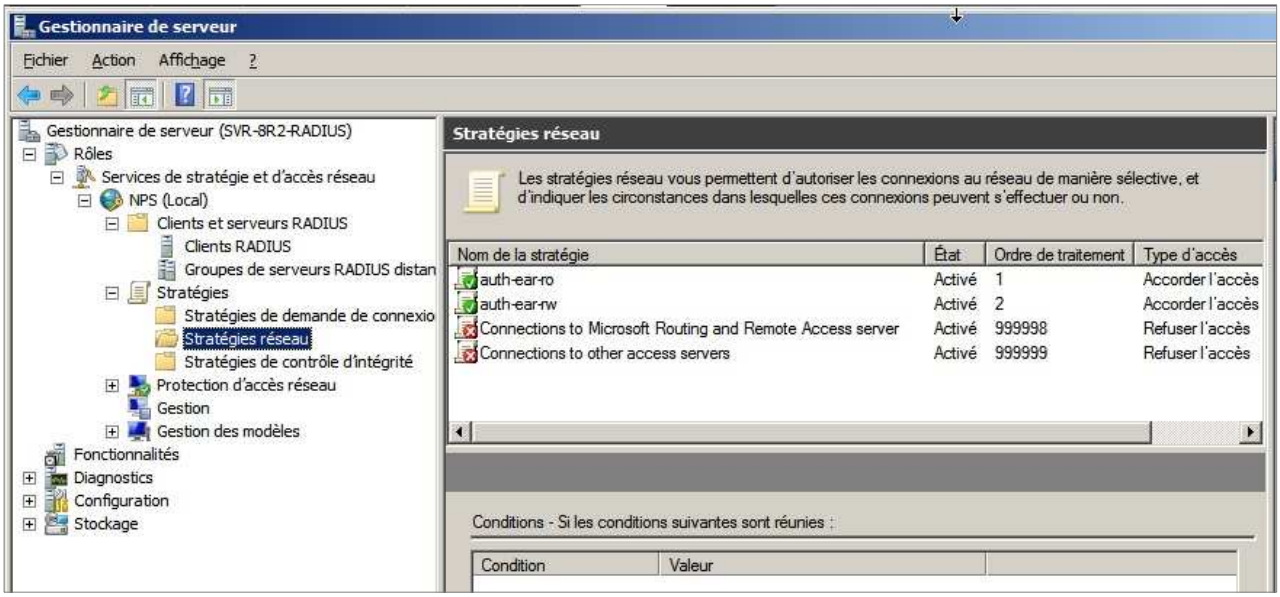
2. Ensuite, il faut inscrire le serveur NPS dans Active Directory. Cette étape va permettre au serveur de s'appuyer sur l'annuaire Active Directory pour authentifier les utilisateurs.



3. L'étape suivante est de paramétrer la liste des clients RADIUS ayant chacun un secret partagé dans le serveur. Ces clients sont les EAR qui vont transmettre les requêtes d'authentification.



4. Enfin, il faut paramétrer les règles d'autorisation qui vont attribuer des droits spécifiques. Dans le cas présent, ces règles sont directement issues de la documentation fournie par constructeur.



Dans le cadre du prototypage, deux règles ont été suffisantes :

- Droits d'administration,
- Droits de consultation.

En effet, la configuration de la gestion des autorisations ne sera pas réalisée lors du prototypage mais pendant la phase de pré-production (cf : § IV3.2 : « Implémentation de la Gestion des autorisations »).

TRAÇABILITE

L'ensemble des éléments constitutifs de la solution retenue ont des fonctions de journalisation. Cependant l'analyse de risque a fait apparaître la nécessité de mettre en place une solution d'agrégation des journaux et de consultation. Ces fonctions ont été regroupées au sein d'un serveur dit de journalisation. Celui-ci va collationner les journaux des différents éléments du système pour les stocker dans une base de données. Le dernier élément du serveur est un outil de consultation des journaux dont le but est de permettre de consulter facilement les journaux.

2.3.3 LA JOURNALISATION

Comme le présente la figure 23, les flux liés à la journalisation sont relativement simples. La journalisation consiste essentiellement à collationner les journaux de tous les éléments, les traiter, les stocker et les présenter au client. L'ensemble se décompose en 5 étapes majeures :

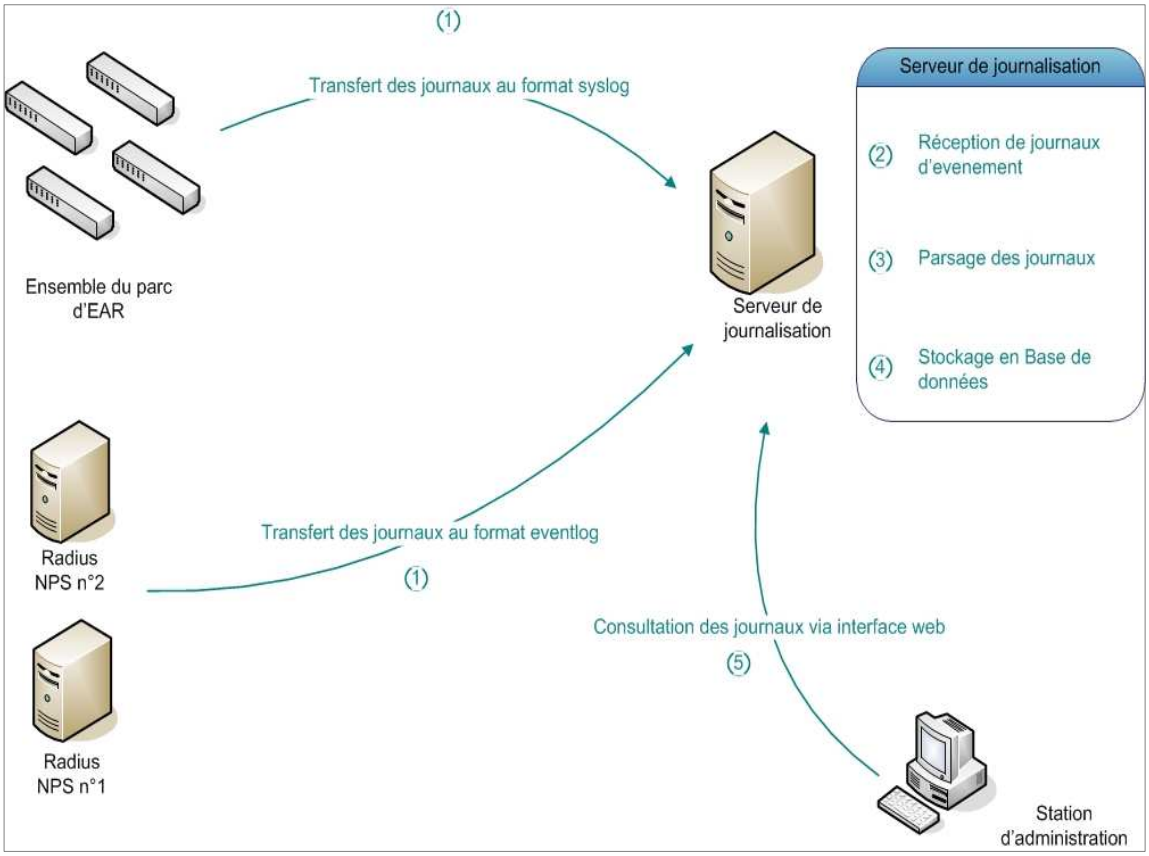


Figure 23 : Fux de journalisation

1. L'ensemble du parc d'EAR renvoient leurs journaux d'événement vers le serveur de journalisation. Les serveurs RADIUS NPS en font de même.
2. Le serveur de journalisation collationne les journaux.
3. Le serveur traite les flux et « parse » les journaux pour pouvoir alimenter la base de données.
4. Les journaux sont stockés en base de données.
5. Les administrateurs peuvent consulter les journaux via une l'interface web

2.3.4 CONFIGURATION DU SERVEUR DE JOURNALISATION

Même si les produits RSYSLOG et LOGANALYZER ont fait l'objet d'une étude comparative lors de la phase de conception (cf. : §III.2 : « Analyse de l'état de l'art »), ils sont néanmoins dépendants d'autres logiciels. Effectivement, le logiciel RSYSLOG fonctionne sur un système Linux et LOGANALYZER est une application web écrite en PHP. Par ailleurs, compte tenu de la quantité de journaux à stocker, il est nécessaire d'utiliser une base de données.

Ces éléments ont donc été sélectionnés en fonction de critères particuliers.

Concernant le système d'exploitation, RSYSLOG étant un produit logiciel fonctionnant sur système Linux, plusieurs possibilités sont envisageables. Mon choix s'est porté sur une distribution sécurisée ayant une forte communauté et disposant de mises à jour régulières (distribution de paquets logiciels récents) : la distribution CENTOS.

Quant au serveur web, CENTOS propose par défaut le serveur APACHE dans les paquets de ses dépôts logiciels. Ce produit possède entre autres, les modules PHP et connecteurs MYSQL nécessaires au logiciel LOGANALYZER. Par ailleurs, il est suffisamment documenté, stable et sécurisé. C'est donc ce produit que j'ai retenu.

Enfin, concernant la base de données, CENTOS propose plusieurs logiciels serveur (entre autres : MYSQL et POSTGRESQL). Du fait de l'existence d'un module pour RSYSLOG permettant de se connecter et d'alimenter une base de données MYSQL, c'est donc ce produit que j'ai sélectionné.

La pile logicielle est donc conforme à celle présentée par la figure suivante :

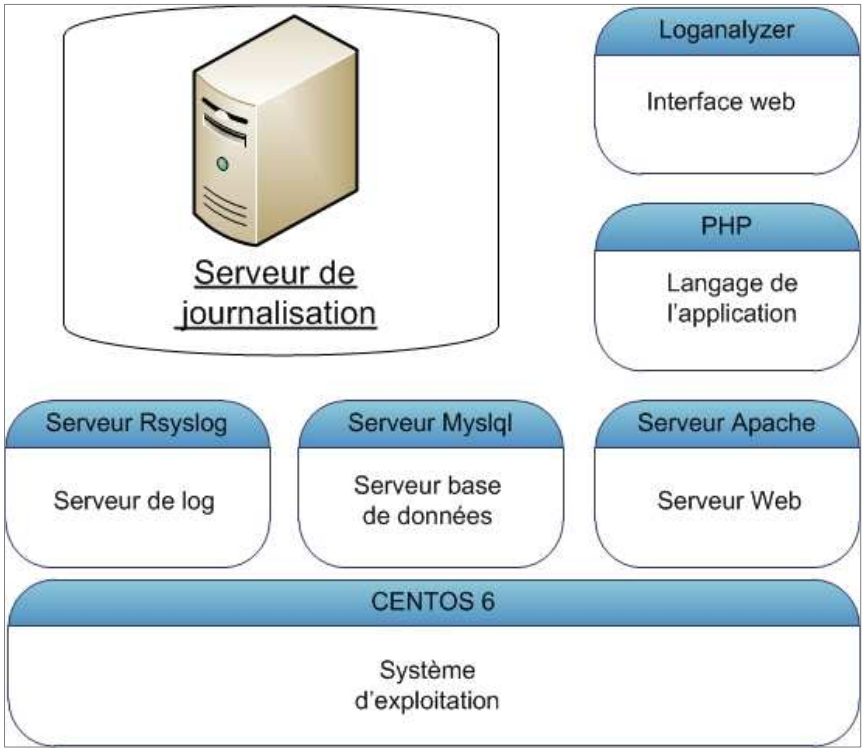


Figure 24 : Pile logicielle du serveur de journalisation

Plus précisément, les versions des composants sont :

- Centos : Version 6
- Mysql : Version 14.14 Distrib 5.1.66 for redhat
- Apache : Version Apache/2.2.15 (Unix)
- Rsyslog : Version 5.8.10
- Loganalyzer : loganalyzer-3.6.3

L'installation et la configuration de la pile logicielle est décrite en **annexe C**.

Chaque applicatif a un rôle précis. La figure 25 présente les interactions logicielles de la pile logicielle du serveur de journalisation :

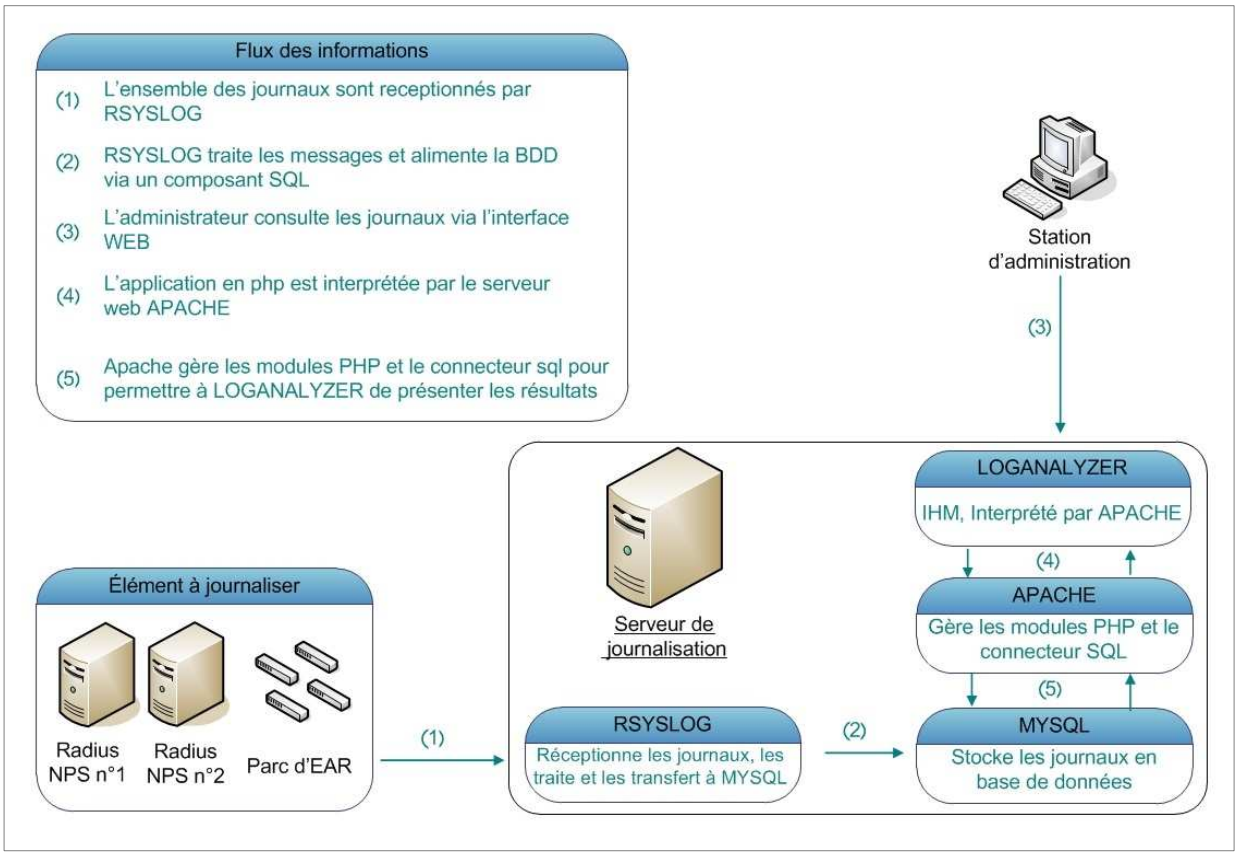
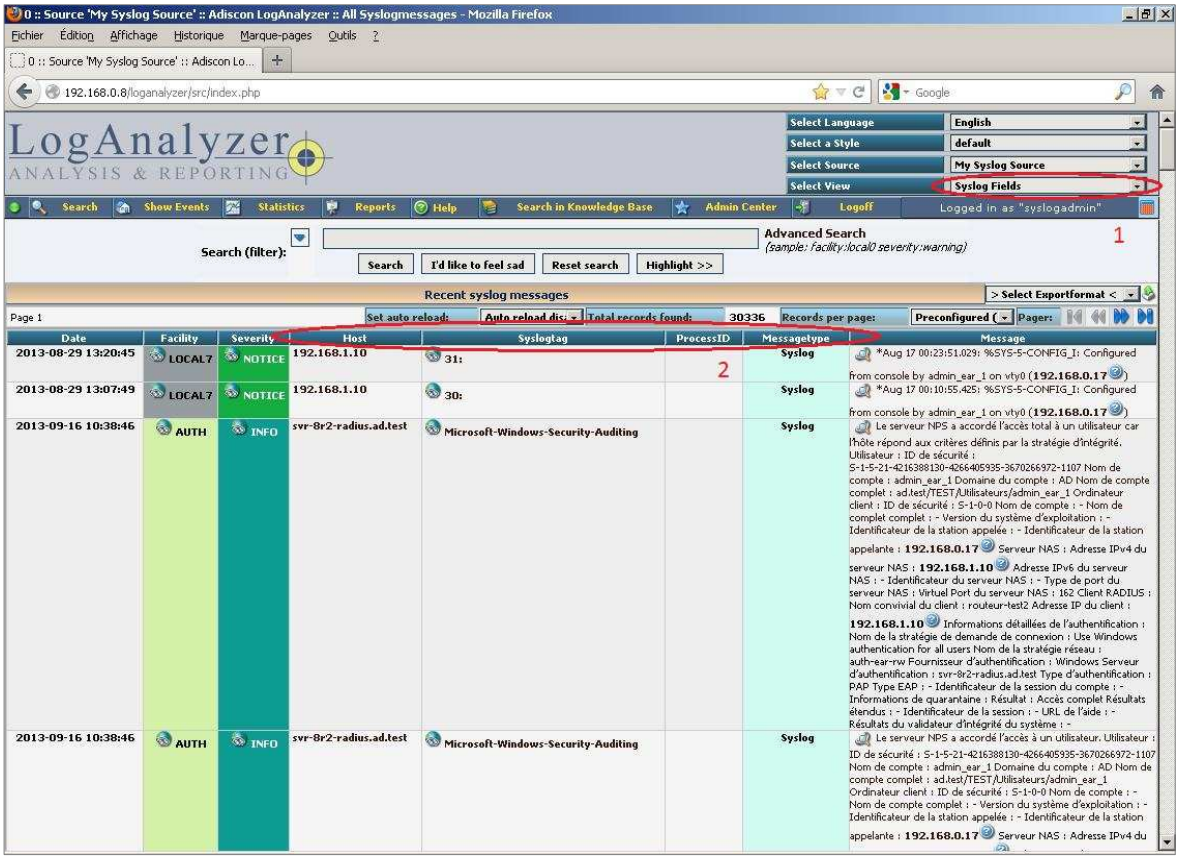


Figure 25 : Traitement des données par le serveur de journalisation

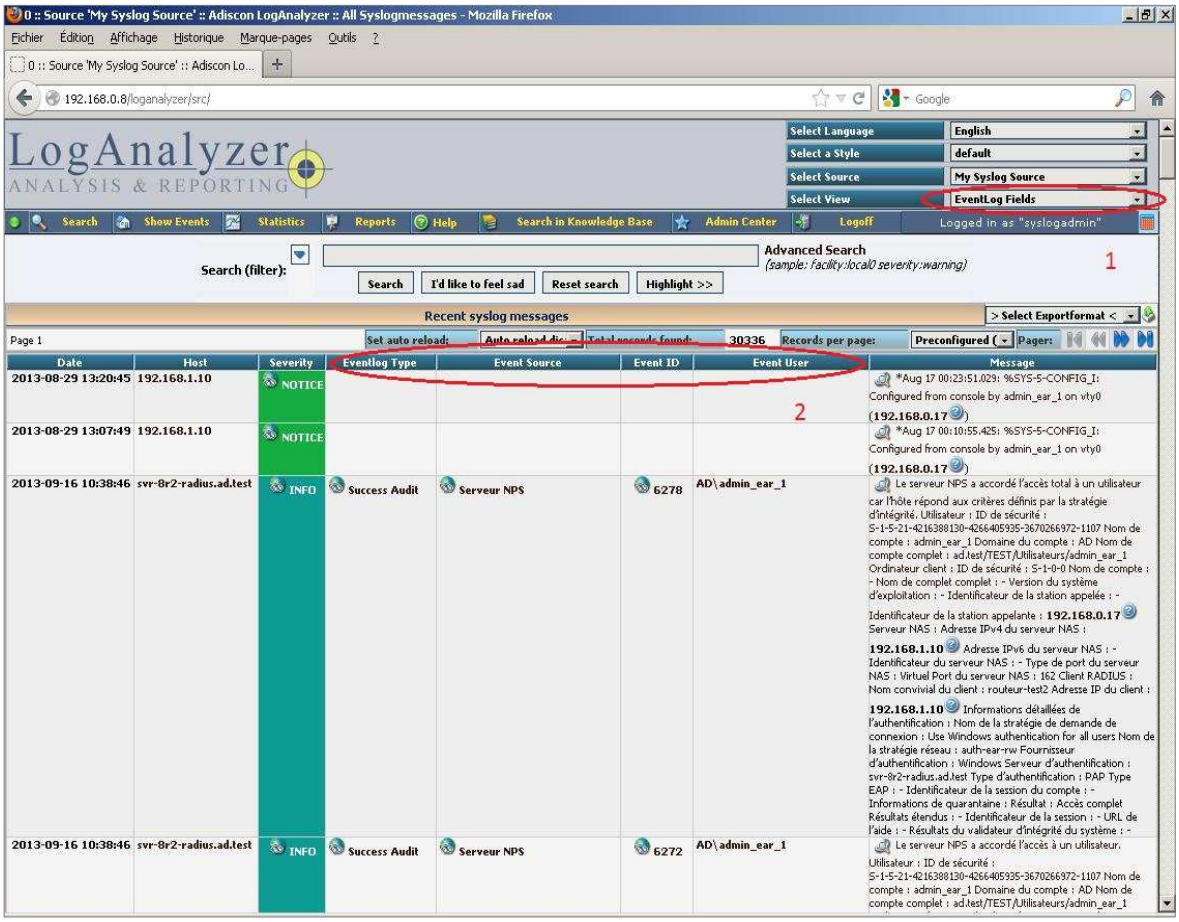
Toute cette pile logicielle est transparente pour l'utilisateur du serveur de journalisation car celui-ci va utiliser l'interface homme-machine web fourni par LOGANALYZER.

Celle-ci est accessible directement depuis un client web. Il est possible de sélectionner les champs à afficher (« 1 ») afin de modifier l'interface ici en (« 2 »). Cela va permettre de favoriser l'étude des journaux EVENTLOG ou SYSLOG en fonction des besoins.

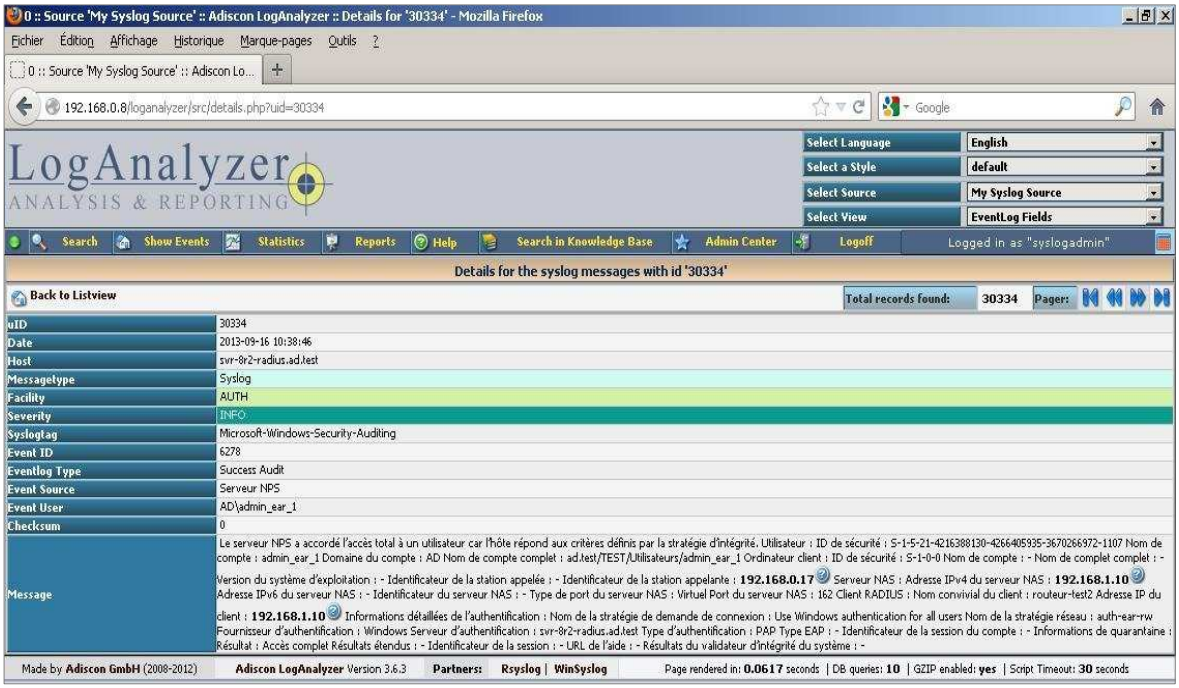
Ci-dessous la « vue » SYSLOG :



Ici la « vue » EVENTLOG :



Il est également possible de détailler un événement en particulier :



2.3.5 CONFIGURATION DES EARS

A l'instar des fonctionnalités d'authentifications RADIUS, les EAR récents disposent d'options de paramétrage des fonctionnalités de journalisation. Il est par exemple possible de filtrer certain types de journaux, de définir les paramètres SYSLOG (facility, priotrity...) et de spécifier un serveur de journalisation.

Dans le cas du projet, le choix a été fait de journaliser l'ensemble des événements et de les conserver un an. Le seul élément de configuration renseigné sera le transfert des journaux vers le serveur de journalisation.

Pour les versions de pré-production et définitive, ce paramétrage restera identique. Cependant, le client prévoit la possibilité ultérieurement de réduire le volume de journaux à transférer en affinant son choix des éléments journalisés.

Dans le cas du prototype, les EAR virtuels étant basés sur des firmwares CISCO, la configuration du transfert de log se fera au travers du menu « logging ».

2.3.6 CONFIGURATION DES SERVEURS NPS

À l'origine, les serveurs Microsoft utilisent le format EVENTLOG comme description des journaux d'évènements. Par ailleurs, aucune option n'est intégrée pour transférer ceux-ci vers un serveur de journalisation, cependant il est possible d'installer un logiciel à cette fin.

Lors de la phase de l'état de l'art (cf. : §III.2.3.1 : « La centralisation des journaux d'événement »), il est apparu que le produit SNARE propose un client Windows gratuit. Ce logiciel répondant aux exigences client, étant configurable et répondant aux besoins du projet, c'est celui-ci que j'ai retenu dans sa version 4.0.1.2a.

Le logiciel est récupérable sur le site du constructeur à cette adresse :

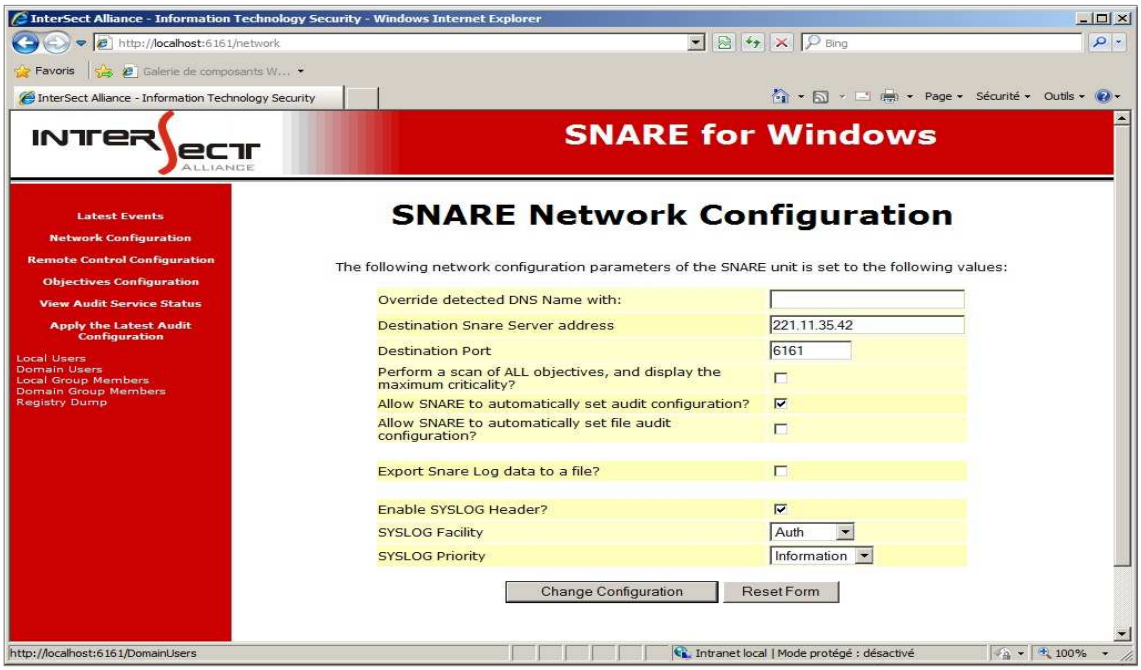
http://www.intersectalliance.com/download.html?link=http://prdownloads.sourceforge.net/snare/SnareForWindows-4.0.1.2a-MultiArch.exe

C'est un exécutable qu'il suffit de lancer pour installer le client de transfert de journaux. Le logiciel s'installe en tant que service et sera lancé automatiquement au démarrage du serveur.

La configuration se fait au travers d'une interface web. Deux éléments principaux sont à configurer :

En premier lieu, les éléments journalisés qui doivent être transférés au serveur de journalisation (ici les requêtes d'authentification ainsi que leurs résultats).

En second lieu, l'adresse du serveur de journalisation ainsi que les éléments de formatage des messages :



Le logiciel s'installant en tant que service, il n'est pas nécessaire de le lancer manuellement. Le transfert des journaux est donc automatique.

Le logiciel propose d'autres options mais elles ne seront pas exploitées dans le cadre de ce projet.

2.4 PROBLEMES RENCONTRES

Lors du développement du prototype, plusieurs problèmes ont été rencontrés. En effet, tous les éléments n'ont pas fournis l'ensemble des fonctions escomptées et/ou ont fait apparaître un dysfonctionnement. Cela concerne plus précisément la configuration de la réplication des serveurs RADIUS (le lot 10) et la configuration de la WebUI LOGANALYZER (le lot 16).

Les problèmes ont chacun été traités différemment. Ces aléas sont expliqués cas par cas ci-dessous.

2.4.1 CONFIGURATION DE LA REPLICATION DES SERVEURS RADIUS

La Configuration de la réplication des serveurs RADIUS (lot 10) a été pensée pour s'appuyer sur la réplication automatique entre produits Microsoft. Or après plusieurs tests, il s'avère que les serveurs NPS de Microsoft n'implémentent pas cette fonctionnalité.

Plusieurs possibilités sont alors envisagées :

- Abandonner le produit NPS au profit d'un produit équivalent qui pourrait implémenter une fonctionnalité de synchronisation,
- Trouver une solution technique permettant une réplication entre deux serveurs RADIUS NPS.

Compte tenu de l'ergonomie du produit Microsoft, de sa facilité d'intégration à l'Active Directory et du temps déjà consacré dessus, c'est la deuxième solution qui a été retenue. Si la fonction de réplication automatique entre deux serveurs NPS n'est pas implémentée nativement dans le produit, il est cependant possible d'exporter les paramètres du serveur RADIUS au format XML ainsi que de les importer. J'ai implémenté cette tâche de manière automatique en m'appuyant sur le langage de script POWERSHELL et une planification de tâche.

Le script de cette configuration est disponible en **annexe D.**

Pour ce qui est de la planification, un « lot 10 bis » a ainsi été intégré au projet et soumis à validation du client. Celui-ci ayant accepté cette alternative, le lot a été développé en suivant le même processus itératif que pour le développement des autres lots.

La planification a évolué pour correspondre à celle décrite ci-après par la figure 26.

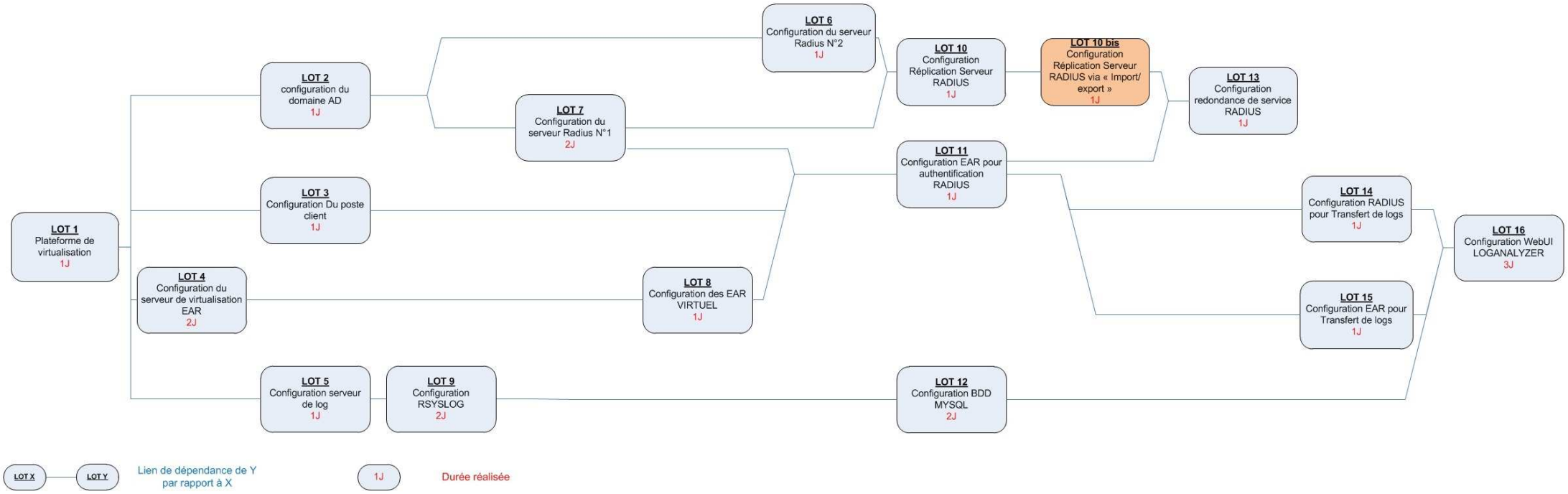


Figure 26 : Planification prototype après adaptation au contexte

2.4.2 CONFIGURATION DE LA WEBUI LOGANALYZER

Lors de la configuration de la WebUI LOGANALYZER (lot 16), un bug d'affichage a été constaté. Celui-ci est directement lié à l'encodage des caractères. Par défaut, les serveurs Microsoft utilisent le codage de caractère CP1252 (très proche de l'ISO-8859-1). Or lorsque l'application web LOGANALYZER doit traiter des données enregistrées en base de données MYSQL dans ce format, rien ne s'affiche.

Plusieurs possibilités sont alors évoquées :

- Changer de produit de consultation et de gestion des logs.
- Modifier les autres éléments de la solution pour s'adapter au produit (Base de données, RSYSLOG, client Windows,…).
- Débuguer le code « Open source » de l'application.

Pour cela, j'ai effectué une matrice des résultats de divers scénarii de configuration des éléments du serveur de journalisation. Il en est ressorti que le format des logs Microsoft doit rester en CP1252, mais que l'application ne peut pas les exploiter.

De plus, au regard du nombre de fonctionnalités liées au produit LOGANALYZER, mon choix a été de conserver cette application.

Une recherche dans le code source a permis d'identifier l'erreur et de procéder à une modification du code. Cette modification du code est décrite dans l'**annexe C**.

Par ailleurs, le bug et la modification proposée ont été signalés à la société mettant à disposition le logiciel (ADISCON) sous la référence 433(Buganalyzer).

À présent, le bug est corrigé depuis la version 3.6.4 du logiciel.

(cf : « http://bugzilla.adiscon.com/show_bug.cgi?id=433 »).

La modification effectuée sur le produit le rendant dès lors pleinement fonctionnel, aucun lot n'a été ajouté au projet. Ce problème à juste induit un glissement des délais (cf. figure 26).

3 INTEGRATION EN ENVIRONNEMENT DE PRE-PRODUCTION

Le prototype a permis au client de valider l'architecture globale de la solution ainsi que son fonctionnement. Il a pu ainsi tester les fonctions d'authentification, de traçabilité et d'autorisation pour un type de matériel particulier (dans ce cas, CISCO).

Une fois le prototype validé par le client, c'est la phase d'intégration en environnement de pré-production qui succède.

La version de pré-production a pour finalité de tester la compatibilité de l'architecture précédemment établie, mais cette fois en environnement de production. Cette phase comporte notamment la configuration et le paramétrage de la fonctionnalité d'autorisation vis-à-vis de chacun des EAR existants.

À l'instar du développement du prototype, cette étape a été décomposée en lots. Ceux-ci ont été priorisés puis traités de manière itérative en collaboration étroite avec le client.

L'architecture de la version de pré-production reste sensiblement identique à celle du prototype. Les seules différences résident dans le fait que :

- l'Active directory est déjà existant
- les stations d'administration sont physiques
- le réseau et les EAR sont physiques et hétérogènes.

Les deux premiers éléments sont peu problématiques dans le sens où ils sont relativement proches du prototype.

Concernant les EAR, leur grande diversité implique que l'activité majeure de cette phase de pré-production, est la configuration des fonctionnalités d'autorisations propres à chaque type de matériel.

3.1 GESTION DE PROJET

La méthodologie de gestion de projet que j'ai utilisé pour le développement du prototype s'étant avérée satisfaisante, j'ai mené le développement de la version de pré-production de la même manière.

3.1.1 DECOMPOSITION ET PLANIFICATION DES TACHES

Le découpage en lots de la phase de pré-production se fait lui aussi sur l'interdépendance des lots entre eux. La figure 27 illustre cette décomposition :

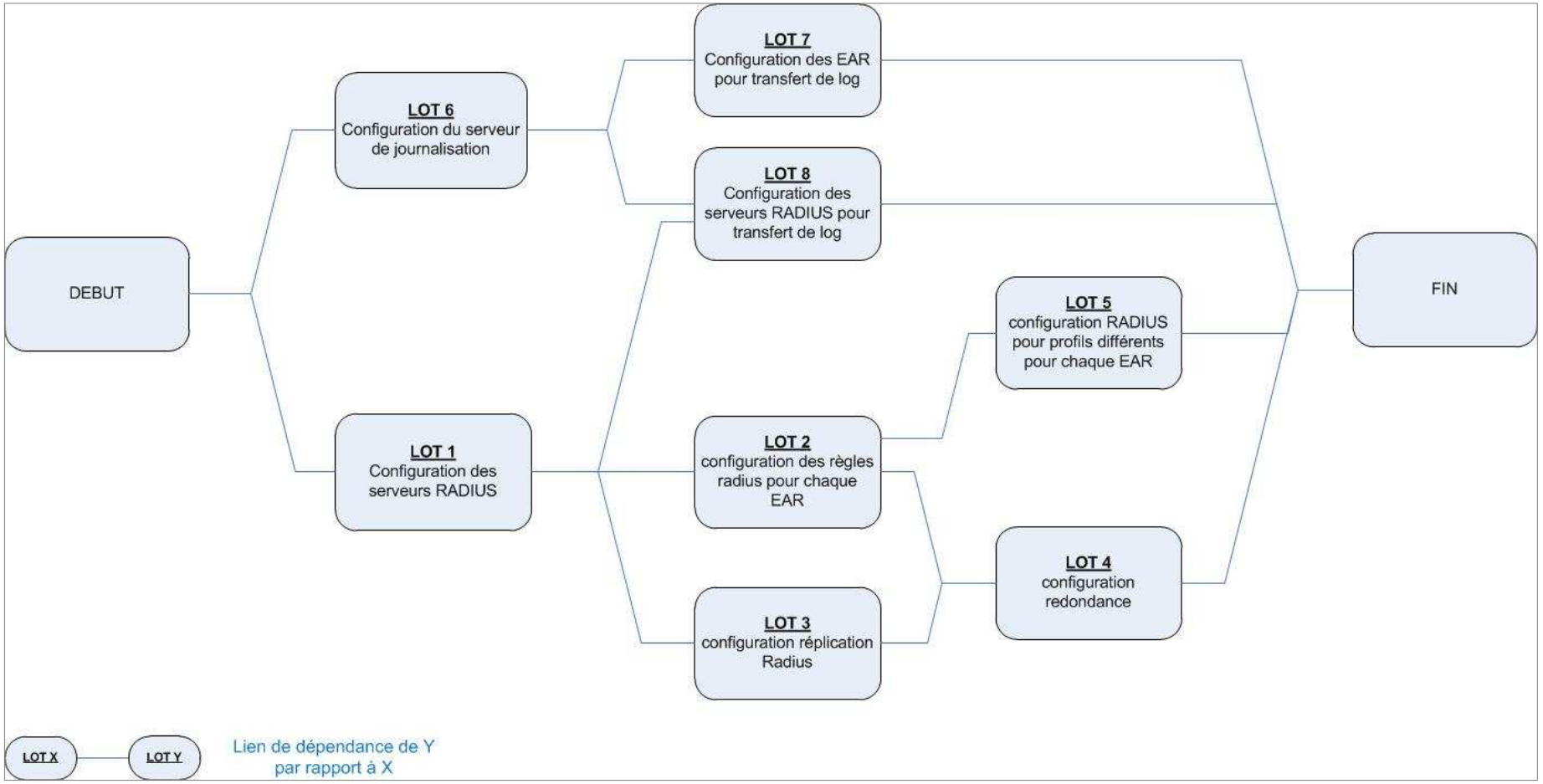


Figure 27: Interdépendance des lots de la pré-production

Toujours en suivant la même méthodologie de projet, des priorités sont fixées sur les différents lots. L'expérience acquise lors de la phase de prototypage m'a permis de réduire certains risques. Les priorités sont donc évaluées en prenant en compte ces éléments. C'est ce que présente la figure 28 ci-dessous :

Descriptif de la Tâche	Numéro de lot	Priorité	Risque
configuration du serveur radius 1	LOT1	1	1
configuration du serveur radius 2			1
configuration du serveur Centos	LOT 6	1	1
configuration de rsyslog			
configuration Mysql			
configuration web UI loganalyzer			
configuration des règles radius pour chaque EAR	LOT 2	2	3
configuration réplication Radius	LOT 3	2	1
configuration EAR pour transfert de log	LOT 7	2	2
configuration radius pour transfert de log	LOT 8	2	1
configuration redondance	LOT 4	3	2
configuration RADIUS pour profils différents pour chaque EAR	LOT 5	3	4

Figure 28 : Evaluation des risques des lots de la version de pré-production.

Les lots ont donc été planifiés tel que le présente la figure 29 :

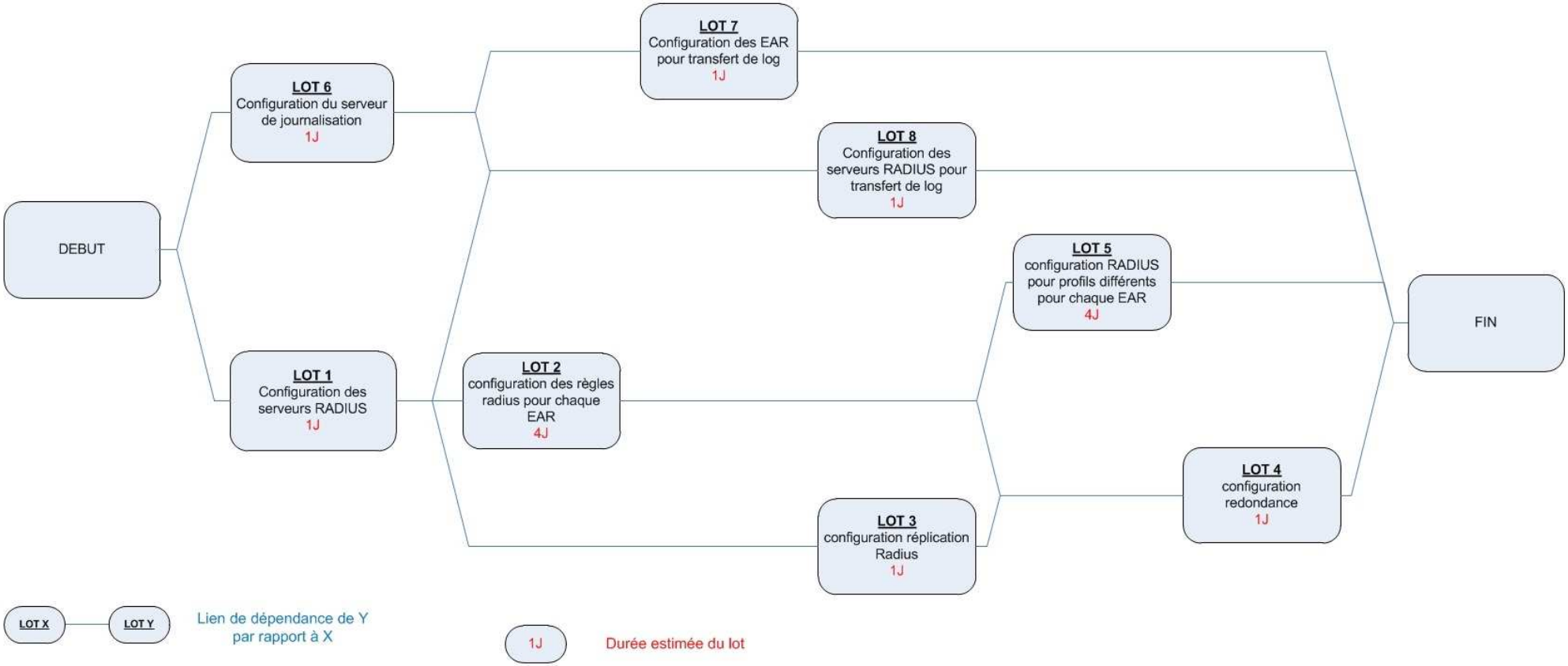


Figure 29 : Planification du développement des composants de la version de pré-production

3.1.2 ADAPTATION AU CONTEXTE

Lors du début de la configuration des règles RADIUS pour chaque EAR (lot 2), il est apparu que le mode opératoire utilisé permettait d'analyser partiellement l'implémentation du protocole RADIUS par les différents équipements.

Or, ce mode opératoire est le même qu'utilisé pour la configuration RADIUS des profils de droits restreints pour chaque EAR (lot 5).

Après réflexion, il s'est avéré que traiter ces deux lots simultanément ne complexifie pas le projet et permet de gagner un temps considérable sur l'ensemble du projet.

Pour gagner en efficacité et en temps, j'ai regroupé ces lots en un lot « 2bis ». Lors de la phase du projet correspondant au lot 2 bis, j'ai donc réalisé la gestion des autorisations différenciées pour chaque équipement. Ainsi, la configuration du serveur RADIUS pour attribuer à l'utilisateur le contrôle total sur un équipement ou bien un accès restreint en fonction de son groupe d'appartenance s'est faite en parallèle.

La planification initiale a alors évolué pour correspondre à celle présentée par la figure 30 ci-dessous :

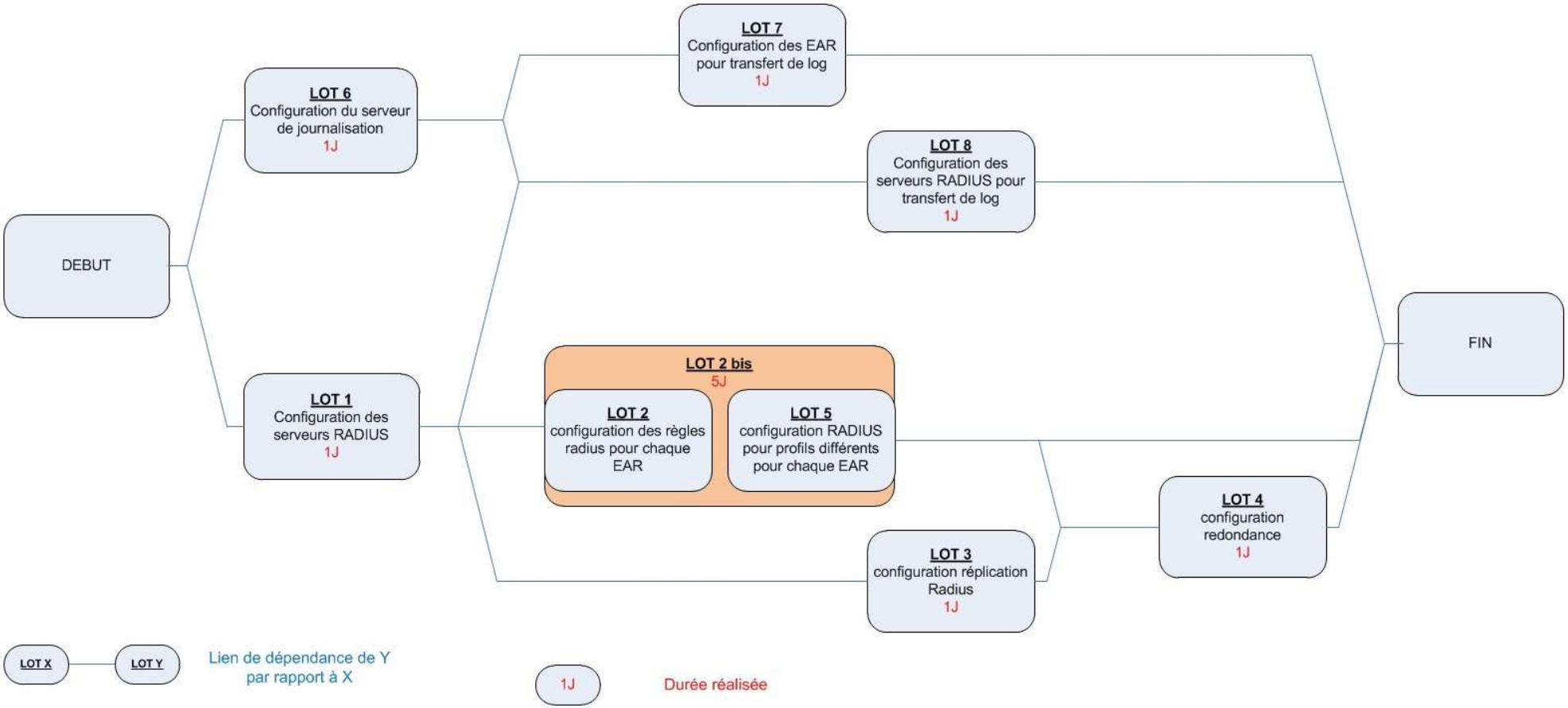


Figure 30 : Planification pré-production après adaptation au contexte.

3.2 IMPLEMENTATION DE LA GESTION DES AUTORISATIONS

Si la phase de prototypage m'a permis de développer et d'architecturer les composants nécessaires aux fonctions d'authentification et de traçabilité, la phase de pré-production a pour objectif principal la configuration des fonctionnalités d'autorisation.

En effet, une fois l'utilisateur authentifié, il est nécessaire de lui accorder des droits particuliers. Ce peut être un contrôle total sur l'équipement auquel il se connecte, ou bien seulement un accès restreint

De par son historique, le parc actuel d'EAR a pour particularité d'être extrêmement diversifié. La gestion des droits étant propre à l'implémentation logicielle de chaque EAR, cet état de fait complexifie la tâche.

Par ailleurs, certains équipements faisant parti des plus vieillissants, n'implémentent pas tout ou partie des prérequis de la solution (SSH et/ou authentification RADIUS). Ils sont alors comptabilisés dans les équipements non compatibles avec la solution implémentée et ne doivent pas dépasser un volume total de 15% (cf. cahier des charges en **annexe B**). Le listing de compatibilité des EAR avec la solution (résultant du travail d'implémentation) est disponible en **annexe D**.

Pour bien maîtriser la gestion des droits, il convient de comprendre comment fonctionne le protocole RADIUS dans la configuration du projet. C'est en prenant en compte ces éléments que le mode opératoire utilisé a été défini.

3.2.1 PROCESSUS D'ADMINISTRATION

Dans le cas présent, comme le présente la figure 31 ci-dessous, l'authentification de l'utilisateur va se faire en 7 étapes. C'est principalement les étapes 2 et 5 (les échanges entre le client RADIUS et le serveur RADIUS) qui vont conditionner la gestion des autorisations.

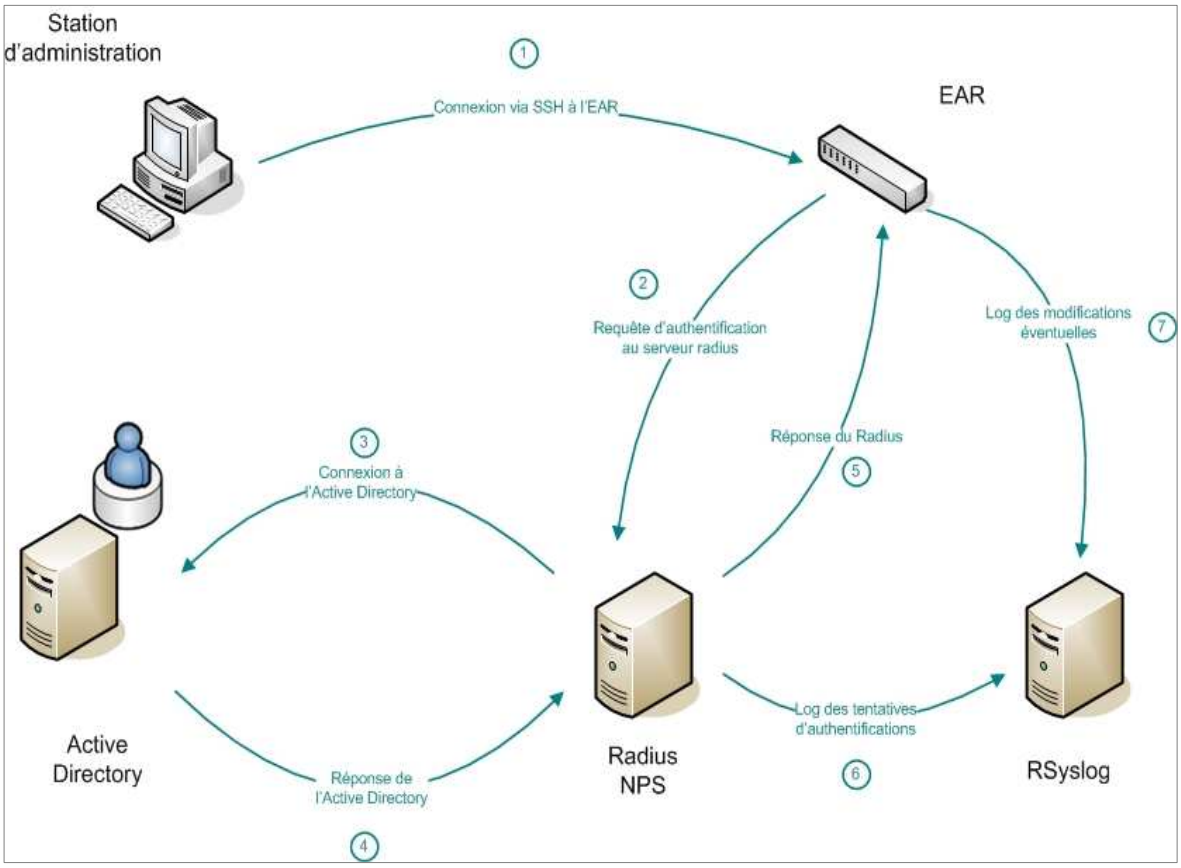


Figure 31 : Etapes d'une session d'administration d'un EAR

1. En premier lieu, l'administrateur se connecte à l'EAR via un canal sécurisé et lui transmet ses informations d'authentification.

2. Ensuite, l'EAR envoie une requête (*Access-Request*) au serveur d'authentification RADIUS via le protocole RADIUS. Il transmet notamment le couple identifiant/mot de passe au serveur, mais peut renvoyer d'autre informations (identifiant fournisseur par exemple).

3. Le serveur RADIUS vérifie ces informations auprès d'un contrôleur de domaine ACTIVE DIRECTORY.

4. Le contrôleur de domaine ACTIVE DIRECTORY renvoie une réponse positive si les informations transmises sont exactes ou négative dans le cas contraire.

5. Le serveur RADIUS renvoie une réponse à l'EAR en fonction de la réussite ou non de l'authentification. La réponse prend la forme d'une « *Access-Reject »* en cas de refus et d'une « *Access-Accept »* en cas de succès. Pour un succès d'authentification, le serveur RADIUS transfère plusieurs Attributs Valeur / Pair (*Attribute Value Pairs*) liés notamment aux autorisations accordées.

6. Le serveur NPS journalise l'authentification sur le serveur de logs.

7. L'EAR journalise les opérations d'authentifications et de modifications sur le serveur de logs.

C’est précisément les attributs Valeur / Pair envoyés par l’EAR au serveur RADIUS lors de l’étape 2 et ceux renvoyés par le serveur lors de l’étape 5 qui vont conditionner les autorisations allouées. En effet, c’est via ces attributs que l’EAR envoie des informations au serveur RADIUS et que ce dernier transmet les éléments d’autorisation propres à chaque EAR.

Ces attributs vont conditionner la gestion des autorisations sur les EARs. Cependant, l’implémentation du protocole RADIUS et de ces attributs en particulier sur les équipements actifs reste quelque peu particulière. Pour bien appréhender la problématique de cette gestion il convient de faire un point sur les éléments constatés.

3.2.2 ARTEFACT CONSTRUCTEURS

Les attributs au protocole RADIUS sont gérés par l’**IANA** (*Internet Assigned Numbers Authority*).

Ils sont répartis selon le tableau suivant :

Range	**Registration Procedures**
1-191	IETF Consensus
192-240	Reserved for private Use
224-240	Implementation Specific
241-246(extended space, Unassigned)	Implementation Specific
241-246(extended space, Reserved)	Standards Action
247-255	Reserved

Par exemple, les 26 premiers attributs de la plage 1 – 191 sont détaillés comme suit :

Valeur	Description
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	**Service-Type**
7	Framed-Protocol
8	Framed-IP-Address
9	Framed-IP-Netmask
10	Framed-Routing
11	Filter-Id
12	Framed-MTU
13	Framed-Compression
14	Login-IP-Host
15	Login-Service
16	Login-TCP-Port
17	Unassigned
18	Reply-Message
19	Callback-Number
20	Callback-Id
21	Unassigned
22	Framed-Route
23	Framed-IPX-Network
24	State
25	Class
26	**Vendor-Specific**
…	…

Certains numéros d'attributs sont réservés et standardisés, d'autres alloués à des fabricants. Chaque constructeur peut ainsi implémenter des fonctions particulières en utilisant l'attribut « Vendor-Specific » (numéro 26).

Ces numéros vont principalement servir lors de l'échange entre le client RADIUS (ici l'EAR) et le serveur RADIUS. Ils fonctionnent selon un principe d'attribut Valeur/pair.

Par exemple, afin d'accorder des droits d'administration sur un équipement, certains fournisseurs vont utiliser des attributs standard tel que « Service-Type » (code d'attribut « 6 »), alors que d'autres vont utiliser des attributs particuliers tels que « Vendor-Specific » (code d'attribut « 26 »).

Service-Type / Administrative

6 6

Vendor-Specific / 3com / 3Com-User-Access-Level / administrator

26 / 43 / 1 / 3

Lors des phases d'analyse, celles-ci ont porté plus particulièrement sur les différents attributs envoyés par les EAR ainsi que les réponses du serveur d'authentification. Il est alors survenu plusieurs cas particuliers.

En premier lieu, plusieurs attributs différents peuvent avoir une même incidence sur un même équipement.

Par exemple, pour reprendre l'exemple des attributs présentés supra, sur les EAR 3COM 5500 les droits d'administration peuvent être accordés selon plusieurs attributs :

Standard : Service-Type Administrative

Spécifique au fournisseur: Vendor-specific/3Com/3

Ensuite, certains matériels renvoient un identifiant constructeur (n° Vendor-Specific) qui n'est pas le leur.

Par exemple, un commutateur H3C 5800 avec le firmware :

H3C Comware Platform Software

Comware Software, Version 5.20, Release 1110P05

Va renvoyer l'identifiant « 2011 » (du constructeur HUAWEI) alors que son identifiant constructeur devrait être le numéro « 25506 »-

Le troisième cas particulier réside dans le fait que deux équipements identiques peuvent renvoyer deux identifiants constructeur différents.

Par exemple, deux commutateurs 3COM 4210, ayant sensiblement la même version de firmware, vont renvoyer des identifiants différents:

L'un, un identifiant H3C :

3Com Switch 4210 26-Port Software Version 3Com OS V3.01.12s56

(vendor specific H3C=25506)

L'autre, un identifiant 3COM

3Com Switch 4210 26-Port Software Version 3Com OS V3.01.13s56

(vendor-specific 3COM=43)

Aussi surprenante soit-elle, cette singularité peut s'expliquer par l'historique des sociétés fabricantes de matériels actifs réseaux.

En effet, la société 3COM a travaillé en partenariat avec la société HUAWEI en 2003 pour créer la société H3C qu'elle a ensuite racheté. Puis 3COM a été entièrement rachetée et intégrée par HP en 2010.

L'explication la plus plausible étant qu'au fil des évolutions des firmwares, les contraintes de production et/ou de compatibilité ont amené les développeurs à conserver du code existant concernant notamment les diverses implémentations du protocole RADIUS.

L'impossibilité de différencier l'implémentation logicielle du protocole en fonction des identifiants constructeurs, a conditionné la gestion des droits. J'ai donc mis en place un mode opératoire spécifique afin de configurer le serveur NPS.

3.2.3 MODE OPERATOIRE

Il a fallu trouver le paramétrage précis pour chaque équipement. Pour cela, les documentations propres à chaque équipement (autrement appelés dictionnaires RADIUS) sont généralement disponibles sur internet.

Par ailleurs, le projet FreeRADIUS collationne un grand nombre de dictionnaires. C'est une source non négligeable d'information pour le paramétrage des autorisations

Cependant, comme cela a été constaté, l'implémentation du protocole RADIUS n'est pas forcément conforme avec les données fournies par le constructeur.

Par ailleurs, du fait que tous les équipements ne spécifient pas forcément leur identifiant constructeur (n° Vendor-Specific) lors de la requête d'authentification (*Access-Request*), il n'est pas possible de spécifier une règle par constructeur. Le choix s'est donc porté sur la réalisation de deux règles globales :

- Une accordant des droits d'administration complets.
- Une accordant seulement des droits de consultation.

Afin de configurer les règles d'autorisation attribuées par le serveur NPS, j'ai procédé comme décrit ci-après :

Le procédé est détaillé dans la figure 32 ci-dessous :

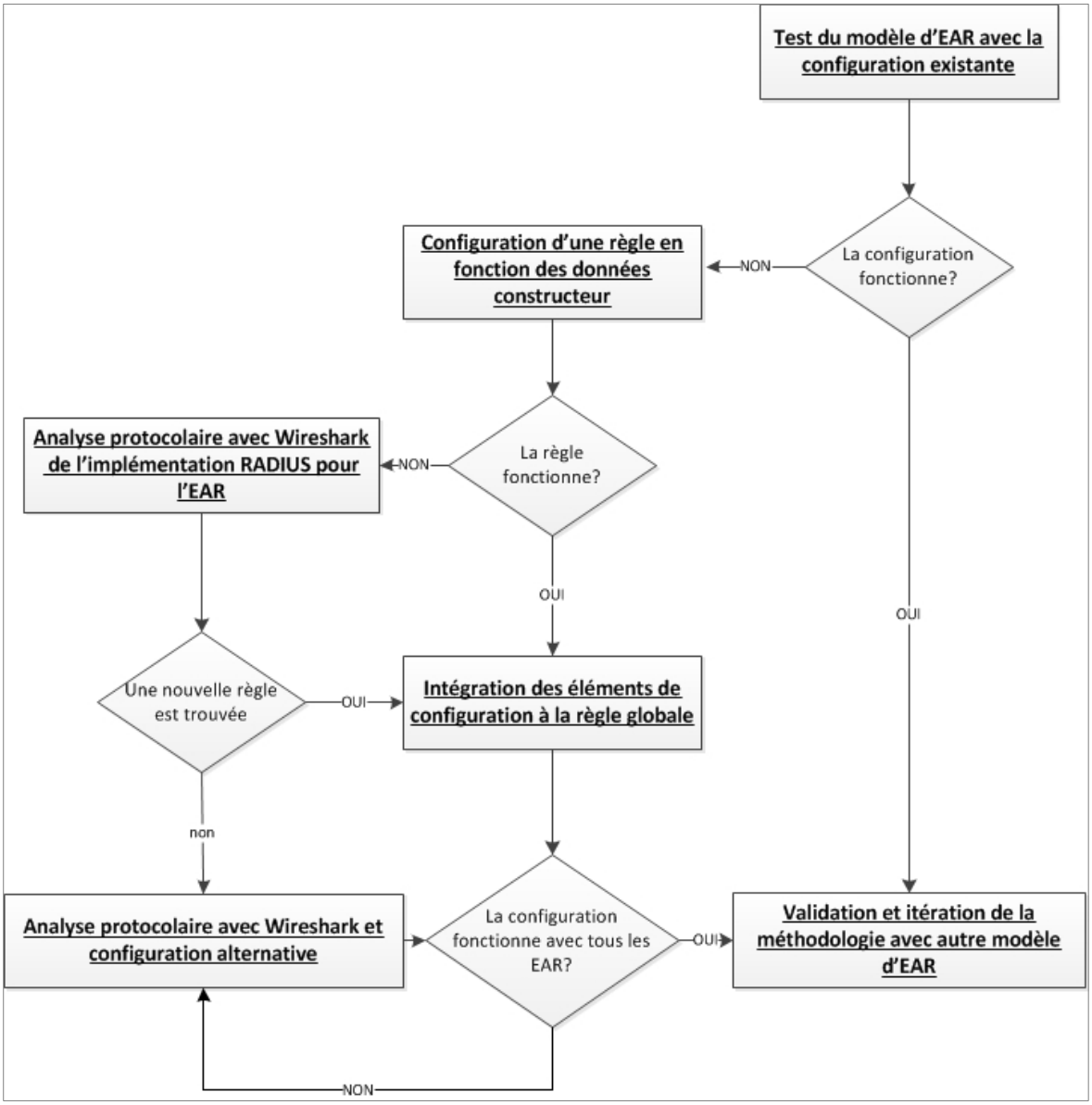


Figure 32 : Méthodologie de configuration du serveur RADIUS

1. En premier lieu, si la configuration globale (règle de base) n'est pas fonctionnelle avec l'équipement en cours de paramétrage, une règle est écrite et testée pour cet équipement en fonction des préconisations constructeur. De cette manière, la configuration est testée individuellement.

2. La règle spécifique est alors intégrée à la configuration globale. Certaines ne sont pas compatibles entre elles. Il faut donc trouver une solution en adaptant la configuration.

3. Ensuite, l'étape suivante est de tester d'autres configurations non documentées. Pour cela, un travail d'analyse du protocole vis-à-vis des différents modèles d'équipements est nécessaire. A cette fin, le logiciel d'analyse de protocole réseau « WIRESHARK » est utilisé. Grâce à ce dernier il est alors possible d'analyser les échanges entre les EARs et le serveur NPS.

4. Enfin les règles sont fusionnées. A chaque ajout d'une nouvelle règle, chaque équipement précédemment configuré est re-testé afin de s'assurer d'une compatibilité totale.

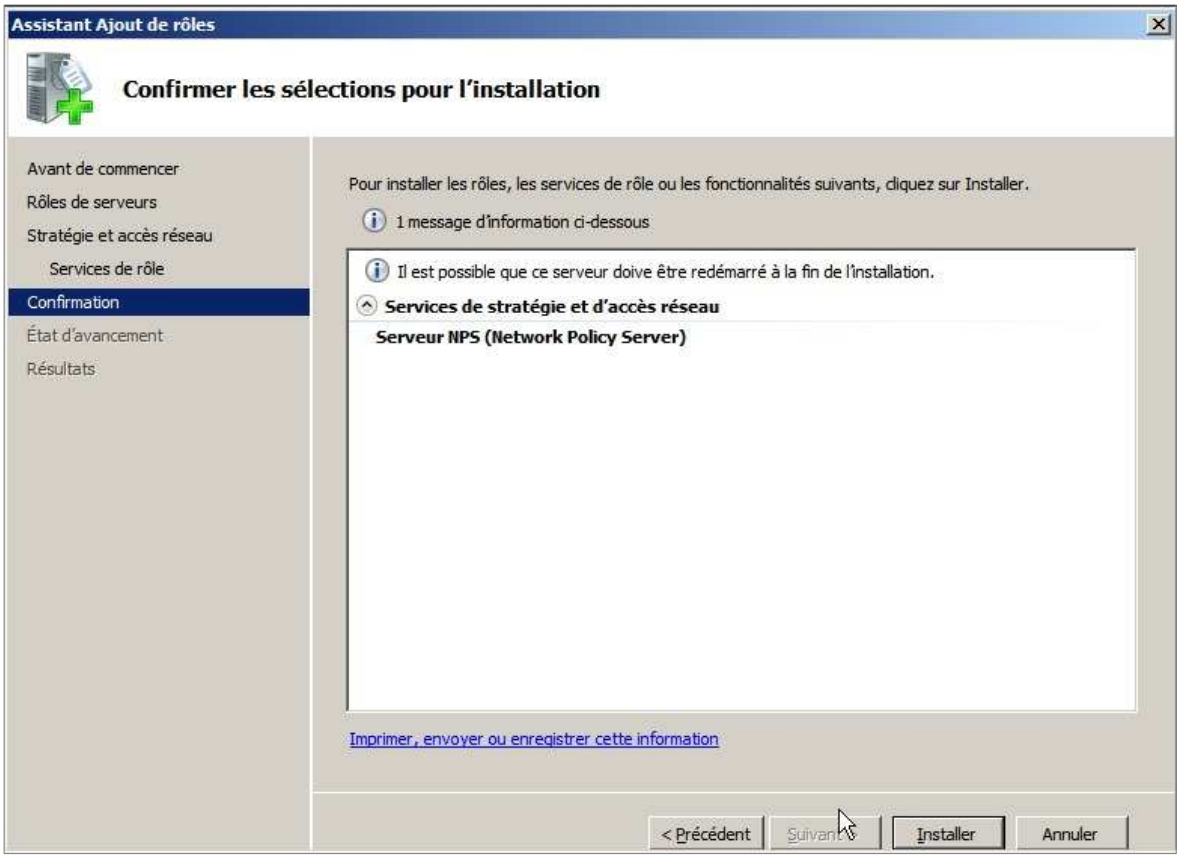
C'est donc ce mode opératoire qui m'a permis de configurer finement la gestion des autorisations sur les serveurs NPS

3.2.4 CONFIGURATION DES SERVEURS NPS

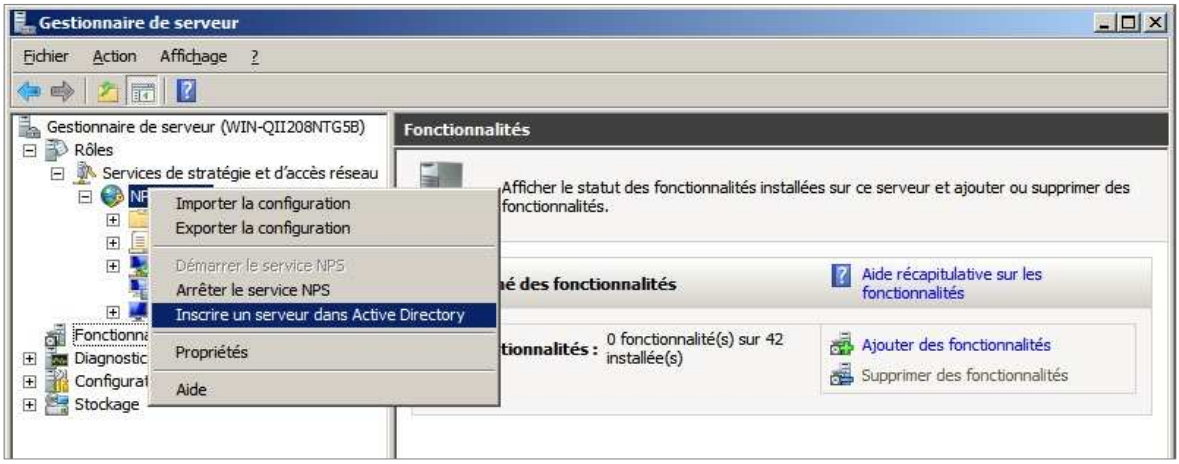
Les serveurs NPS sont relativement simples à mettre en place. La gestion des autorisations représente le point le plus compliqué, c'est pourquoi le mode opératoire a été précisé supra.

- Pour cela, il faut tout d'abord installer Windows serveur 2008 R2 « Enterprise » sur une machine (serveur principal).

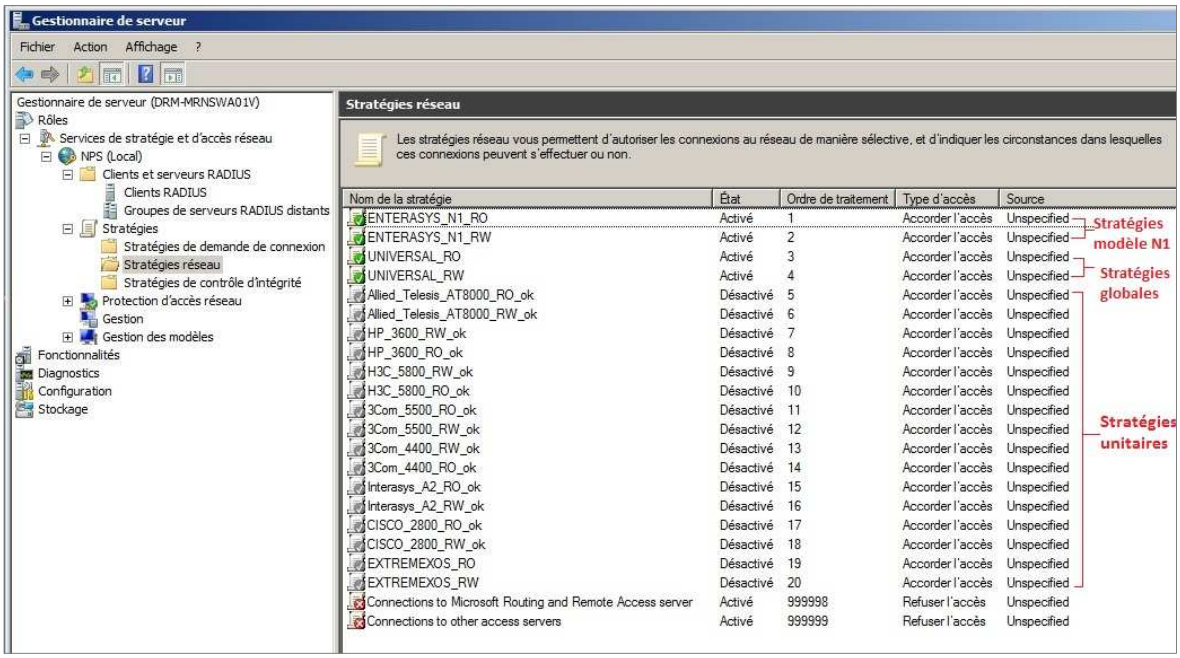
- Ensuite, il faut rajouter parmi les rôles de « Services de stratégie et d'accès réseau » celui de « Serveur NPS (Network Policy Server) ».



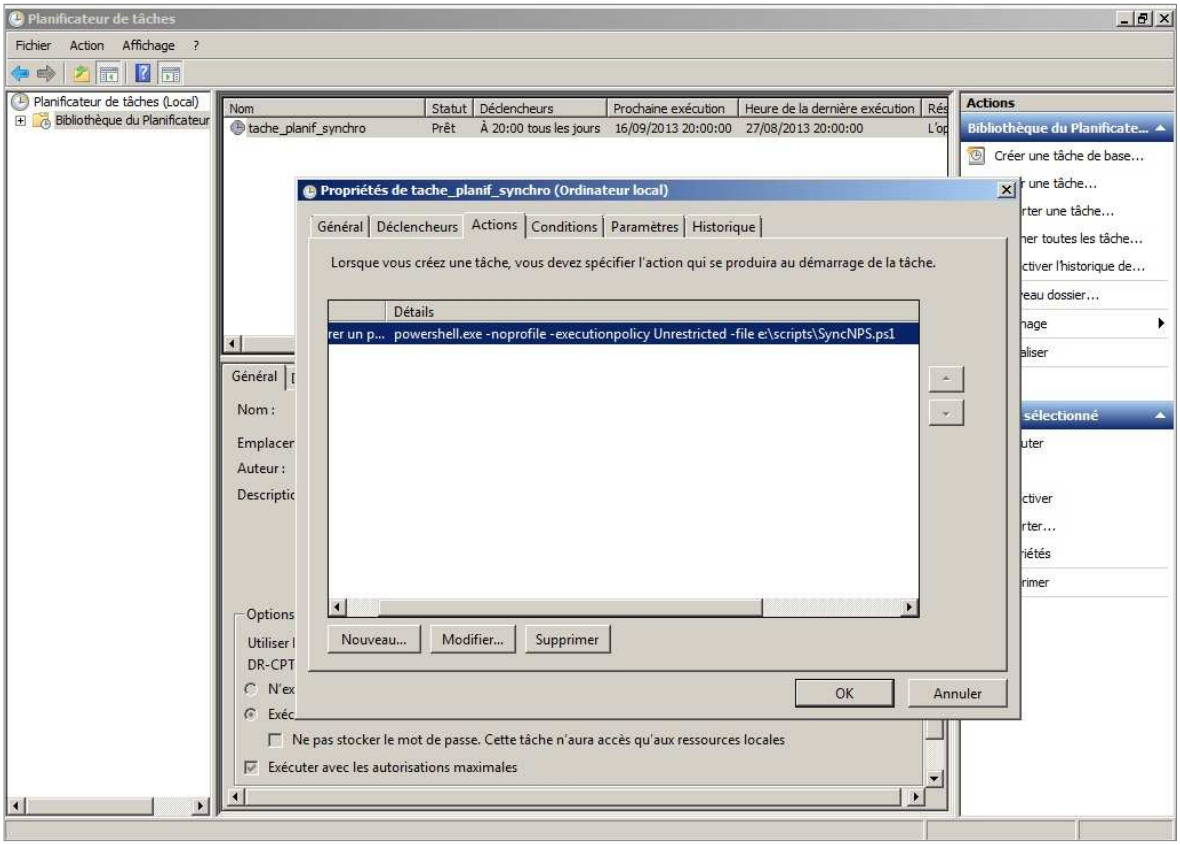
- L'étape suivante consiste à intégrer le serveur dans le domaine et « inscrire le serveur (NPS) dans Active Directory ». Cette étape va permettre au serveur NPS de s'appuyer sur la base de compte Active Directory pour l'authentification.



- Puis, il convient de mettre en œuvre le mode opératoire décrit supra afin de configurer les règles du serveur NPS (la configuration des stratégies effectives est détaillée en **annexe E**). Ci-dessous la vue des stratégies réseau :



- La dernière étape consiste à configurer la réplication sur le serveur NPS secondaire. Pour cela, les services (« Services de stratégie et d'accès réseau » notamment celui de « Serveur NPS (Network Policy Server) ») doivent être déployés sur le réplica. Enfin il faut planifier l'exécution régulière du script Power Shell adéquat. Celui-ci est disponible en **annexe F**.



Les serveurs NPS ainsi que leur réplication sont maintenant paramétrés. Il reste désormais à configurer l'authentification RADIUS sur les EARs.

3.2.5 CONFIGURATION DES EARS

La configuration des EAR est propre à chaque équipement. Cependant, le principe général reste commun. Il s'agit de paramétrer l'EAR au travers d'un menu dédié en pour permettre l'obtention des autorisations depuis un serveur RADIUS.

Pour reprendre l'exemple du routeur CISCO 3745, la configuration de la gestion des autorisations va se faire simplement telle que le décrit la figure 33ci-après

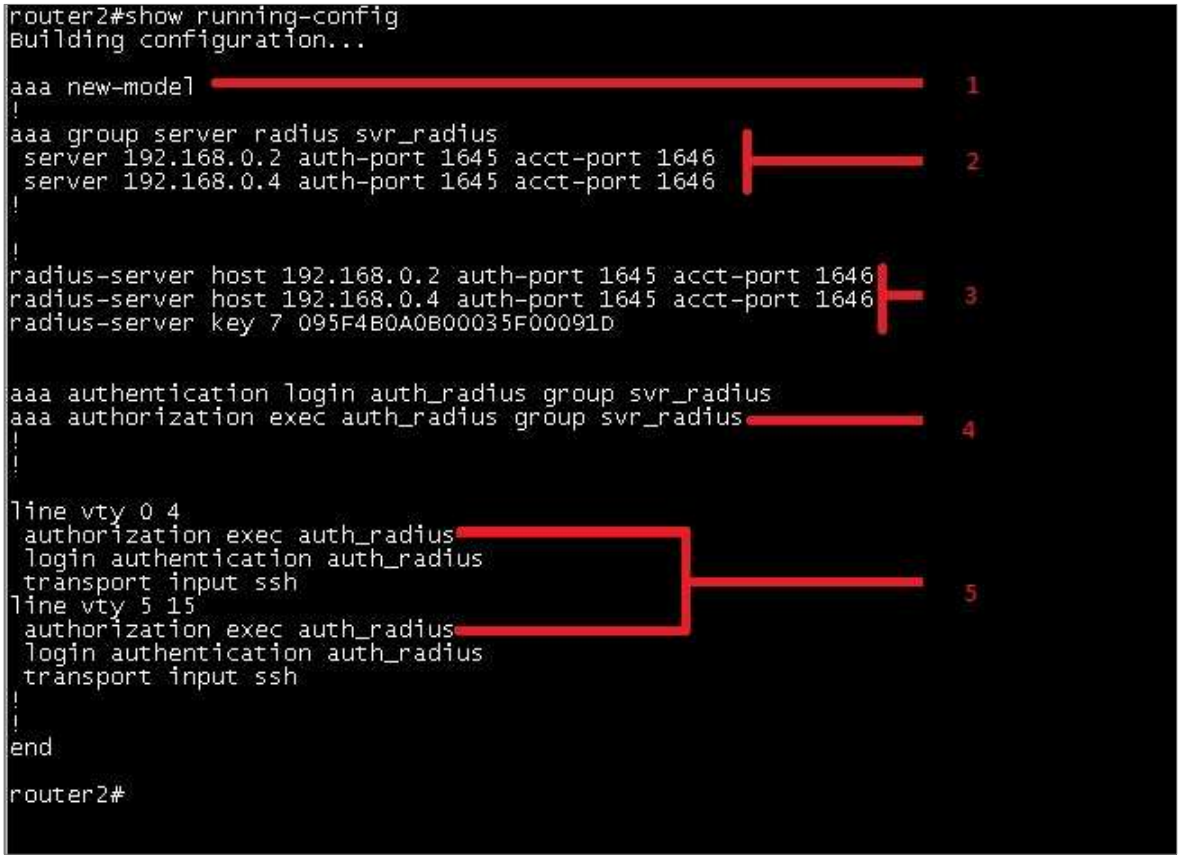


Figure 33 : Configuration gestion des autorisations RADIUS sur un EAR CISCO

1. Créer un nouveau model AAA. Ce sera le cadre général du paramétrage des fonctionnalités AAA de l'EAR.
2. Définir les serveurs RADIUS. Chaque serveur RADIUS est déclaré ainsi que les ports de communication utilisés s'ils ne sont pas standards. Une clef secrète est paramétrée pour chiffrer les échanges avec les serveurs.
3. Définir un groupe serveur RADIUS qui regroupera l'ensemble des serveurs RADIUS.
4. Déclarer un mode d'autorisation AAA s'appuyant sur le groupe RADIUS créé.
5. Paramétrer la gestion des autorisations et l'attribution de droits à ouverture de session sur les consoles virtuelles. Ces dernières doivent se baser sur les informations renvoyées par le serveur RADIUS.

Les étapes 1 à 3 sont identiques à celles pour configurer l'authentification. Il n'est pas nécessaire de les répéter.

4 VALIDATION

4.1 LE CAHIER DES CHARGES

Le client a volontairement été fortement impliqué à la phase de réalisation du projet, afin de développer un produit ayant le maximum de conformité avec ses exigences.

En outre, ce mode de gestion de projet a permis de faire valider les différents éléments au fur et à mesure de leur implémentation.

La phase de recette n'a donc pas été uniquement réalisée à la « fin » du projet mais s'est étalée tout au long de celui-ci. Du fait de son implication, le client a pu juger en temps réel de l'avancée du développement des fonctionnalités ainsi que de leur conformité à ses attentes.

En premier lieu, le prototype a permis de valider principalement les éléments relatifs à l'authentification et la journalisation de la solution. Ainsi, le client a pu tester la solution dans un environnement simplifié. Il a pu constater le fonctionnement global de la solution et son ergonomie. L'architecture globale a alors été validée

L'intégration en environnement de production a complexifié la solution en enrichissant la solution de multiples contraintes. A ce titre, tous les éléments ayant été approuvés pour le prototype ont été configurés pour prendre en compte l'environnement existant.

La version de pré-production a donc permis au client d'évaluer la solution dans une version directement éligible à la production.

Concernant plus particulièrement les exigences 65, 66 et 67 (cf **annexe B** « Cahier des charges »), sur lesquelles le client a insisté, elles ont été traitées comme suit :

- Exigence 65 : La solution doit permettre de réduire de min 66% le temps consacré aux changements des mots de passe.

  Le client n'a plus de mots de passe à changer sur l'ensemble des éléments compatibles. Les EAR non compatible représentent moins de 34% du parc, le temps nécessaire aux changements de mots de passe est donc réduit de plus de 66%.

- Exigence 66 : La solution doit permettre à un groupe d'utilisateurs restreint (max 20 pax) de mettre en œuvre la PSSI en vigueur.

  L'objectif est largement rempli dans le sens où une seule personne peut mettre en œuvre la solution utilisable par un grand nombre d'utilisateurs.

- Exigence 67 : La solution doit être compatible avec min 85% du parc d'équipements actifs.

  Seule une petite partie du parc n'est pas compatible avec l'ensemble de la solution (essentiellement des matériels de marque Allied Telesis). Ces éléments sont principalement des matériels anciens prévus d'être renouvelés. Il s'avère qu'en l'état actuel des choses, cette part correspond à moins de 15% du volume du parc.

  La solution pourrait donc tendre vers une compatibilité proche des 100% dans un avenir proche.

Le cahier des charges a donc été validé dans son intégralité, d'une part de manière unitaire au fur et à mesure du déroulement du projet et d'autre part dans sa globalité à la fin de celui.

4.2 RETOUR SUR LES OBJECTIFS

Pour rappel, les objectifs initiaux du projet étaient de trois ordres :

- Fonctionnels : Le projet visait à mettre en place une solution d'administration des EAR qui permette de s'adapter aux réorganisations et réductions de personnels.
- Economiques : Les coûts de mise en place devaient être faibles et ceux d'exploitation réduits par rapport à la situation existante.
- Sécuritaires : Le niveau de sécurité de la fonctionnalité d'administration des EARs devait s'améliorer.

Concernant les **objectifs fonctionnels**, la solution actuelle permet notamment de gérer facilement deux types de profils d'utilisateurs :

- Administrateurs
- Consultants

Cela permet à une équipe restreinte de manager la sécurité des EARs. En effet, il n'est plus besoin de changer les mots de passes des équipements régulièrement. Cette fonctionnalité est transférée à l'Active Directory qui l'implémente déjà.

La gestion des droits et autorisations passant maintenant par l'appartenance à un groupe Active Directory, il est très facile d'attribuer ou de retirer des droits à une personne, sans compromettre la sécurité. Effectivement, il suffit de faire appartenir un utilisateur à un groupe approprié ou au contraire de l'y exclure.

Auparavant, le « Turn over » de personnels du centre de service aurait impliqué de modifier trop régulièrement les mots de passes locaux, ce qui excluait la possibilité de déléguer certaines tâches sans affaiblir la sécurité.

Cela explique qu'il est maintenant possible de déléguer une partie des fonctions (consultations) au centre de service (ex : consultation d'un équipement pour savoir si un port est bien configuré).

En termes d'**objectifs économiques**, la réduction de la charge de travail liée à l'administration de la sécurité permet en premier lieu de dégager du temps aux équipes d'administration pour d'autres tâches.

Ensuite, la possibilité de déléguer au centre de service des fonctions de consultation permet à celui-ci de diagnostiquer et éventuellement traiter certains problèmes simples et/ou non liés aux EAR. Le temps d'intervention est ainsi réduit, chaque équipe est valorisée et la qualité de service augmente (notamment pour l'utilisateur).

Enfin, en ce qui concerne les **objectifs de sécurité**, le niveau de sécurité s'est vu grandement amélioré. En effet plusieurs éléments sont à noter :

- La mise en place d'une solution d'authentification centralisée s'appuyant sur l'Active directory.
- La suppression de l'obligation de modifier régulièrement les mots de passe sur chaque EAR (à charge de chaque utilisateur de l'Active Directory).
- La centralisation des journaux d'événement ainsi que la possibilité de les consulter par une interface web.

Ces éléments sont les principaux mais des effets transverses sont aussi notables. Par exemple, la réduction du nombre de mots de passes réduit les probabilités pour qu'un utilisateur les note sur un papier quelconque.

Le projet répond effectivement aux objectifs stratégiques fixés par le client.

V CONCLUSION

Pour conclure, la solution apportée par ce projet a su répondre aux attentes du client tant vis-à-vis du cahier des charges que des objectifs de celui-ci.

Il reste maintenant à le valoriser et prévoir ses perspectives d'évolution.

1 VALORISATION

La version de pré-production a donc été validée par le client. Les tests ont montrés qu'elle est directement exploitable telle quelle au sein de la zone de responsabilité du CIRISI Rennes.

Cependant, le contexte et l'organisation du soutien des SI étant en pleine évolution, le déploiement a été reporté à une date ultérieure par le client.

En effet, certaines prérogatives pourraient prendre une ampleur nationale. L'authentification sur les équipements actifs réseau est l'une d'entre elles.

1.1 AU SEIN DE LA REGION NORD-OUEST

La solution issue du projet est exploitable immédiatement. Néanmoins, il est fort probable que les serveurs déployés ne soient pas ceux de la version de pré-production car cette dernière a été préalablement prévue pour être supprimée après validation.

Le client souhaite mettre en place la solution par lui-même afin de mettre en œuvre les documentations d'installation et de configuration livrées.

La configuration ainsi que le paramétrage de la version de production seront donc identiques à la version de pré-production.

Par ailleurs, une réorganisation au niveau national pourrait donner une autre dimension au projet.

1.2 AU NIVEAU NATIONAL

La chaîne de soutien des SI du ministère de la défense possède une chaîne de valorisation et d'amélioration continue. Tout projet peut être signalé via un dossier à un bureau spécialisé à la direction centrale afin d'être étudié. Un dossier de valorisation est en cours auprès de la direction centrale.

La valorisation au niveau national pourrait se faire au travers d'une délégation de missions nationales (administration des serveurs d'authentification), au profit du client.

Le projet aurait alors une mise en œuvre de dimension nationale.

2 PERSPECTIVES

2.1 AXES D'AMELIORATION

En l'état actuel des choses, le principal problème de compatibilité de la solution est lié à l'hétérogénéité du parc d'EAR. Ce point va se résoudre au fur et à mesure du remplacement des matériels vieillissant au profit de matériels plus récents. Par ailleurs, la gestion des EAR n'étant plus dévolue à des équipes locales mais à une cellule nationale, la cohérence du parc devrait s'en voir accrue.

Ensuite, l'accroissement du nombre d'EAR va induire une charge de trafic et traitements.

L'architecture pourra évoluer afin d'implémenter des serveurs Radius proxy qui permettront de mieux répartir la charge liée à cette évolution.

Par ailleurs, l'axe principal d'amélioration réside dans la collation et l'exploitation des journaux d'événements.

Le serveur de journalisation répond aux besoins actuels mais n'est pas adapté à un SOC (*Security Operations Center*). Une solution de corrélation et d'analyse permettrait d'améliorer la sécurité.

3 NOTES PERSONNELLE

Pour mener à bien ce projet et produire une solution en adéquation avec les attentes du client, j'ai dû d'une part structurer et organiser mon activité, et d'autre part développer de nouvelles compétences. Par ailleurs, plusieurs contraintes et problèmes sont survenus tout au long du projet auxquels mon expérience personnelle et professionnelle m'a permis de m'adapter. Au final, le fait que le client mette en œuvre ma solution sur sa zone de compétence (le quart nord-ouest de la France) et souhaite la déployer sur l'ensemble du territoire français, me conforte dans mes choix.

Dans une autre mesure, outre la solution réalisée pour répondre à la problématique du client, ce projet est avant tout l'aboutissement de plusieurs années de travail au CNAM. J'ai la satisfaction d'avoir suivi ce cursus d'ingénieur des Arts et Métiers, lequel m'a permis d'acquérir les savoirs, savoir-faire et savoir-être faisant de moi l'ingénieur que je suis.

VI ANNEXES

ANNEXE A : ANALYSE DE RISQUES

Une analyse des biens essentiels (fonctions et informations) nécessaires à la fonction de télé-administration, va permettre de décomposer ceux-ci en biens supports. Une étude des menaces, vulnérabilités et impact permettra de définir les risques et de définir les besoins en termes de Disponibilité, d'Intégrité et de confidentialité. Les objectifs de sécurité seront spécifiés en fonction des résultats obtenus à partir des critères communs.

Entités – Fonctions - Informations

Entités	**Matériels**		**Logiciels**						**Rso**	**Organisation**	**Sites**
	Machine cliente d'administration	Baie serveurs	Bases d'authentification locales aux EAR	Protocole de télé-administration (SSH)	Application destockage des MDP	Infrastructure de virtualisation	Serveur de fichiers	Serveur d'application	Réseau Ethernet	DEX/RZO	Local : salle serveur
Fonctions											
Configuration des équipements	X	X	X	X	X	X		X	X	X	X
Sauvegarder les configurations	X	X	X	X	X	X	X	X	X	X	X
Informations											
Mots de passe		X	X		X	X		X			X
Plan adressage IP		X				X	X				X
plan de l'architecture		X				X	X				X
Configuration EAR		X				X	X				X
Carnet fils		X				X	X				X

Synthèse des besoins de sécurité

Fonctions		D	I	C
Intitulé	**Description**			
Configuration des équipements	La possibilité de modifier la configuration d'un équipement.	3	3	2
Sauvegarder les configurations	La possibilité d'effectuer une sauvegarde d'un Equipement Actif Réseau	1	3	2

Informations		D	I	C
Intitulé	**Description**			
Mots de passe	Les mots de passes sont nécessaires à toute action de configuration et/ou de sauvegarde	3	3	2
Adresses IP	Adresses des équipements et des réseaux IP	1	2	2
plan de l'architecture	Plan de l'architecture physique du réseau et adressage	2	2	2
configuration EAR	Configuration des Equipements Actifs Réseaux	2	3	2
Carnet fils	Plan de brassage des bâtiments	1	2	2

Classification maximum	3	3	2

Critère/valeur	4	3	2	1	0
Disponibilité	H24	Sous 2H	Sous 8H	Sous 48H	Sous 1 semaine
Intégrité	Maximale	Très forte	Moyen	Faible	Faible
Confidentialité	Secret Défense	Confidentiel Défense	Confidentiel Spécifique	Diffusion restreinte	Information ouverte

Menaces

Thème	Menaces	Accidentelle	Délibérée	Ludique	Avide	Stratégique	Terroriste
I Accidents physiques	01 – incendie	X	X	X			X
	02 – dégâts des eaux	X	X	X			X
	03 – pollution						
	04 – accidents majeurs	X					
II Evènements naturels	05 – phénomène climatique						
	06 – phénomène sismique						
	07 – phénomène volcanique						
	08 – phénomène météorologique	X					
	09 - crue						
III Perte des services essentiels	10 – défaillance de la climatisation	X	X	X			
	11 – perte d'alimentation énergétique	X	X	X			X
	12 – perte des moyens de télécommunication	X	X	X			X
IV Perturbations dues aux rayonnements	13 – rayonnements électromagnétiques						
	14 – rayonnements thermiques						
	15 – impulsion électromagnétique (IEM)						
V Compromission des informations	16 – interception de signaux parasites compromettants						
	17 – espionnage à distance						
	18 – écoute passive						
	19 – vol de supports ou de documents		X		X		
	20 – vol de matériels		X		X		
	21 – divulgation interne		X	X			
	22 – divulgation extérieure		X	X	X		
	29 – informations sans garantie de l'origine						
	30 – piégeage du matériel						
	31 – utilisation illicite du matériel						
	33 – piégeage du logiciel						
	39 – abus de droit		X	X	X		

	40 – usurpation de droit		X	X	X		
	42 - fraude						
VI Défaillance technique	23 – panne matérielle	X					
	24 – dysfonctionnement matériel	X	X	X			
	25 – saturation du matériel	X					
	26 – dysfonctionnement logiciel	X					
	28 – atteinte à la maintenabilité du SI						
VII Agression physique	27 – destruction de matériels	X	X	X			
VIII Actions illicites	30 – piégeage du matériel						
	33 – piégeage du logiciel						
	39 – abus de droit		X	X	X		
	40 – usurpation de droit		X	X	X		
	41 – reniement d'actions		X		X		
	42 - fraude						
IX Compromission des fonctions	20 – vol de matériel		X		X		
	25 - saturation	X					
	28 – atteinte à la maintenabilité du SI						
	30 – piégeage du matériel						
	31 – utilisation illicite du matériel						
	32 – altération du logiciel	X	X	X	X		
	33 – piégeage du logiciel						
	34 – copie frauduleuse de logiciel						
	35 – utilisation de logiciels contrefaits ou copiés						
	36 – altération des données	X	X	X	X		
	39 – abus de droit		X	X	X		
	40 – usurpation de droit		X	X	X		
	41 – reniement d'actions		X		X		
	42 - fraude						
	43 – atteinte à la disponibilité du personnel	X					
X Erreur	37 – erreur de saisie	X					
	38 – erreur d'utilisation	X					

Synthèse des menaces

Menace	Risques	D	I	C
01 – incendie	Détérioration du matériel	3		
	Perte de données	3		
02 – dégâts des eaux	Détérioration du matériel	3		
04 – accidents majeurs	Détérioration du matériel	3		
	Perte de données	3		
08 – phénomène météorologique	Arrêt complet du système (foudre)	3		
10 – défaillance de la climatisation	Arrêt complet du système	2		
11 – perte d'alimentation énergétique	Arrêt complet du système	2		
12 – perte des moyens de télécommunication	Impossibilité de transmettre des données	3		
19 – vol de supports ou de documents	Disparition des données avec possibilité de diffusion à des personnes non autorisées			2
20 – vol de matériels	Vol de matériels attractifs	3		2
21 – divulgation interne	Accès aux données par des personnes non autorisées et interne à l'institution			1
22 – divulgation extérieure	Accès aux données par des personnes non autorisées et externe à l'institution			1
23 – panne matérielle	Interruption de service	3	2	
24 – dysfonctionnement matériel	Matériel n'effectuant pas correctement les fonctions prévues	3	2	
25 – saturation du matériel	Système bloqué ou fonctionnant en mode dégradé	2	1	
26 – dysfonctionnement logiciel	Système effectuant des actions non-conformes	3	3	
27 – destruction de matériels	Matériel hors service	3		
32 – altération du logiciel	Le logiciel effectue des traitements non prévu	3	3	
36 – altération des données	Les informations sensibles sont modifiées	3	4	2
37 – erreur de saisie	Insertion de données erronées dans le système		4	

	Transfert de données par des moyens inappropriés ou à un mauvais destinataire			**2**
38 – erreur d'utilisation	Faire effectuer au système des actions non souhaitées	**2**	**2**	
39 – abus de droit	Accès à des données ou des fonctions non autorisées	**2**	**2**	**1**
40 – usurpation de droit	Recherche de pouvoirs d'un niveau supérieur à ce qui est prévu		**1**	**3**
41 – reniement d'actions	Défaut d'imputabilité		**2**	
43 – atteinte à la disponibilité du personnel	Un ou plusieurs personnels ne peuvent travailler	**2**		

La sévérité s'exprime sur une échelle de 0 à 4 selon la graduation suivante :
• 0 : impact nul ;
• 1 : impact faible (négligeable) ;
• 2 : impact moyen (sensible, dommageable) ;
• 3 : impact grave (critique, grave) ;
• 4 : impact extrême (stratégique, inacceptable).
Pour la confidentialité :
• 0 : information ouverte ;
• 1 : diffusion restreinte ;
• 2 : confidentiel spécifique ;
• 3 : confidentiel défense ;
• 4 : secret défense.

Synthèse des risques

Menace	Risques	Impact maximum			Mesure		
		D	I	C	Catégorie	T	NT
01 – incendie	Détérioration du matériel	3			2		X
	Perte de données	3			2		X
02 – dégâts des eaux	Détérioration du matériel	3			2		X
04 – accidents majeurs	Détérioration du matériel	3			2		X
	Perte de données	3			2		X
08 – phénomène météorologique	Arrêt complet du système (foudre)	3			1		X
10 – défaillance de la climatisation	Arrêt complet du système	2			2		X
11 – perte d'alimentation énergétique	Arrêt complet du système	2			2		X
12 – perte des moyens de télécommunication	Impossibilité de transmettre des données	3			2		X
19 – vol de supports ou de documents	Disparition des données avec possibilité de diffusion à des personnes non autorisées			2	2	X	
20 – vol de matériels	Vol de matériels attractifs	3		2	2	X	
21 – divulgation interne	Accès aux données par des personnes non autorisées et interne à l'institution			1	1	X	
22 – divulgation extérieure	Accès aux données par des personnes non autorisées et externe à l'institution			1	2	X	
23 – panne matérielle	Interruption de service	3	2		2	X	
24 – dysfonctionnement matériel	Matériel n'effectuant pas correctement les fonctions prévues	3	2		2	X	
25 – saturation du matériel	Système bloqué ou fonctionnant en mode dégradé	2	1		2	X	
26 – dysfonctionnement logiciel	Système effectuant des actions non-conformes	3	3		2	X	

27 – destruction de matériels	Matériel hors service	**3**			**2**	**X**	
32 – altération du logiciel	Le logiciel effectue des traitements non prévu	**3**	**3**		**2**	**X**	
36 – altération des données	Les informations sensibles sont modifiées	**3**	**4**	**2**	**2**	**X**	
37 – erreur de saisie	Insertion de données erronées dans le système		**4**		**2**	**X**	
	Transfert de données par des moyens inappropriés ou à un mauvais destinataire			**2**	**3**	**X**	
38 – erreur d'utilisation	Faire effectuer au système des actions non souhaitées	**2**	**2**		**2**	**X**	
39 – abus de droit	Accès à des données ou des fonctions non autorisées	**2**	**2**	**1**	**1**	**X**	
40 – usurpation de droit	Recherche de pouvoirs d'un niveau supérieur à ce qui est prévu		**1**	**3**	**2**	**X**	
41 – reniement d'actions	Défaut d'imputabilité		**2**		**2**	**X**	
43 – atteinte à la disponibilité du personnel	Un ou plusieurs personnels ne peuvent travailler	**2**			**1**	**X**	

Vulnérabilité

Menace	Vulnérabilité	Matériels	Logiciels	Réseau	Organisation	Sites
01 – incendie	Manque de cohérence des mesures contre l'incendie					0,25
	Absence de consignes				0,25	
02 – dégâts des eaux	Canalisation d'eau à proximité du système					0,25
	Structure du bâtiment					0,25
04 – accidents majeurs	Possibilité de destruction par collision (chute d'aéronef,…)					0,25
08 – phénomène météorologique	Absence de protection contre la foudre					0,25
10 – défaillance de la climatisation	Arrêt intempestif de la climatisation (panne, sabotage...)					0,25
11 – perte d'alimentation énergétique	Panne du groupe électrogène pendant coupure EDF					0,25
12 – perte des moyens de télécommunication	Dysfonctionnement du réseau externe (destruction,)			0,25		
	Facilité d'accès aux équipements actifs réseaux					0,25
	Défauts d'exploitation du réseau (défaillance)			0,5		
19 – vol de supports ou de documents	Facilité de pénétrer sur le site ou les locaux					0,25
	Manque de vigilance				0,25	
	Absence de règles morales ou d'éthique				0,25	
20 – vol de matériels	Matériel attractif	0,5				
	Facilité de pénétrer dans les locaux					0,25
	Absence de prise en compte du matériel					0,25
	Absence de règles morales ou d'éthique				0,25	

21 – divulgation interne	Non-respect des procédures de transfert (non utilisation du chiffrement)				0,5	
	Peu de sensibilisation aux problèmes de sécurité				0,25	
	Obtention d'un avantage					
	Personnel manipulable					
22 – divulgation extérieure	Non-respect des procédures de transfert (non utilisation du chiffrement)				0,5	
	Peu de sensibilisation aux problèmes de sécurité				0,5	
	Obtention d'un avantage				0,5	
	Personnel manipulable				0,5	
	Non-respect du devoir de réserve				0,25	
	Facilité de divulgation d'information vers l'extérieur de l'organisme				0,25	
23 – panne matérielle	Fiabilité des ressources	0,5		0,5		
	Défaut de maintenance	0,5		0,5		
	Mauvaises conditions d'utilisation	0,5		0,5		
	Absence de consignes relatives à l'utilisation du matériel				0,5	
24 – dysfonctionnement matériel	Possibilité de mal configurer ou installer	0,5		0,5		
	Ressources insuffisamment recettées	0,5		0,5		
	Usure du matériel	0,5		0,25		
25 – saturation du matériel et du réseau	Ressources mal dimensionnées	0,25		0,5		
	Possibilité d'un nombre trop important de requêtes	0,25		0,25		
26 – dysfonctionnement logiciel	Mauvaise installation ou conception des logiciels		0,25	0,25		
	Mauvaise gestion des versions et configurations			0,25		

	Dysfonctionnements dus aux caractéristiques du réseau			0,25		
27 – destruction de matériels	Fragilité des matériels	0,25	0,5			
	Mauvaise utilisation des matériels	0,25				
	Personnel peu soigneux				0,25	
32 – altération du logiciel	Possibilité d'altération par un virus ou un ver informatique (effets malicieux)	0,5	0,5	0,5		
	Possibilité de modifier ou changer les ressources (Télé-administration)	0,25	0,25	0,25		
36 – altération des données	Modification erronée d'une information		0,25			
37 – erreur de saisie	Personnel peu habitué à la saisie				0,5	
	Conditions de travail défavorables				0,5	
	Absence de motivation pour les travaux associés à la saisie (ou surchargés)				0,5	
38 – erreur d'utilisation	Matériel d'utilisation complexe ou peu ergonomique	0,5		0,5		
	Personnel peu ou mal formé				0,5	
	Absence de formation sur les matériels ou logiciels utilisés	0,5	0,5		0,5	
39 – abus de droit	Absence de règles morales ou d'éthique				0,25	
	La notion de droit n'est pas définie pour le personnel				0,25	
	Absence de définition du droit d'en connaître				0,25	
	Prééminence de la catégorie de personnel				0,25	
40 – usurpation de droit	Absence de règles morales ou d'éthique				0,5	
	Absence d'habilitation du personnel				0,25	
	Possibilité d'utiliser les ressources sans contrôle		0,25	0,25		
41 – reniement d'actions	Système accessible et utilisable par tous	0,25	0,25	0,25		0,25
	Traitement nécessite une intervention	0,5	0,25			

	humaine					
	Système accessible sans identification et authentification	0,25	0,25			0,25
43 – atteinte à la disponibilité du personnel	L'ensemble des personnels se blessent ou tombe malades simultanément				0,25	
	Surcharge de travail dans les activités				0,25	

Sévérité des risques

Menace	Faisabilité Vraisemblance	Max (DIC)	Poids : (Fais x Max)	
01 – incendie	0,25	3	0,75	D
02 – dégâts des eaux	0,25	3	0,75	D
04 – accidents majeurs	0,25	3	0,75	D
08 – phénomène météorologique	0,25	3	0,75	D
10 – défaillance de la climatisation	0,25	2	0,5	D
11 – perte d'alimentation énergétique	0,25	2	0,5	D
12 – perte des moyens de télécommunication	0,5	3	1,5	D
19 – vol de supports ou de documents	0,25	2	0,5	C
20 – vol de matériels	0,5	3	1,5	D
21 – divulgation interne	0,5	1	0,5	C
22 – divulgation extérieure	0,5	1	0,5	C
23 – panne matérielle	0,5	3	1,5	D
24 – dysfonctionnement matériel	0,5	3	1,5	D
25 – saturation du matériel et du réseau	0,5	2	1	D
26 – dysfonctionnement logiciel	0,25	3	0,75	D + I
27 – destruction de matériels	0,5	3	1,5	D
32 – altération du logiciel	0,5	3	1,5	D + I
36 – altération des données	0,25	4	1	I
37 – erreur de saisie	0,5	4	2	I
38 – erreur d'utilisation	0,5	2	1	D + I
39 – abus de droit	0,25	2	0,5	D + I
40 – usurpation de droit	0,5	3	1,5	C
41 – reniement d'actions (imputabilité)	0,5	2	1	I
43 – atteinte à la disponibilité du personnel	0,25	2	0,5	D

Synthèse

37 – erreur de saisie	0,5	4	2	I
12 – perte des moyens de télécommunication	0,5	3	1,5	D
20 – vol de matériels	0,5	3	1,5	D
23 – panne matérielle	0,5	3	1,5	D
24 – dysfonctionnement matériel	0,5	3	1,5	D
27 – destruction de matériels	0,5	3	1,5	D
32 – altération du logiciel	0,5	3	1,5	D + I
40 – usurpation de droit	0,5	3	1,5	C
25 – saturation du matériel et du réseau	0,5	2	1	D
36 – altération des données	0,25	4	1	I
38 – erreur d'utilisation	0,5	2	1	D + I
41 – reniement d'actions (imputabilité)	0,5	2	1	I

Note	**Faisabilité**	**Probabilité**
0	Menace totalement infaisable	Menace improbable
0,25	La menace nécessite des moyens très importants ou des connaissances élevées.	La menace est faiblement probable.
0,5	La menace nécessite un certain niveau d'expertise ou du matériel spécifique.	La menace est moyennement probable.
0,75	La menace est réalisable avec des moyens standards ou des connaissances de base.	La menace est fortement probable.
1	La menace est réalisable par tout public.	La menace est certaine.

Habilitation et mode d'exploitation

Habilitation minimum des personnels		
Confidentialité	**Intégrité**	**Disponibilité**
3	3	3
Mode d'exploitation		
Confidentialité	**Intégrité**	**Disponibilité**
2 (dominant)	2 (dominant)	2 (dominant)

	Confidentialité	**Intégrité**	**Disponibilité**
0	Pas d'habilitation	Modification non autorisée	Mise à disposition non autorisée
1	Habilitation minimale	Certains droits de modification sur une partie du système cible	Mise à disposition à priorité faible
2	Habilitation spécifique	Tous les droits de modifications sur une partie du système cible	Mise à disposition à priorité moyenne
3	Confidentiel défense	Certains droits de modification sur tout le système cible	Mise à disposition à priorité forte
4	Secret défense	Tous les droits de modification sur tout le système cible	Mise à disposition à priorité immédiate

Classe ITSEC

Disponibilité	Mode d'exploitation		Classification maximum des informations			
			1	2	3	4
Niveau d'habilitation minimum des utilisateurs	0	1				
		2				
		3	F-Q2	F-Q2	F-P1	F-P3
	1	1	N			
		2	F-Q2			
		3	F-Q2	F-Q2	F-P1	F-P3
	2	1	N	N		
		2	F-Q2	F-Q2		
		3	F-Q2	F-Q2	F-P1	F-P2
	3	1	N	N	N	
		2	F-Q2	F-Q2	F-Q2	
		3	F-Q2	F-Q2	F-P1	F-P2
	4	1	N	N	N	F-Q2
		2	F-Q2	F-Q2	F-Q2	F-Q2
		3	F-Q2	F-Q2	F-P1	F-P1

Confidentialité	**Mode d'exploitation**	↘	**Classification maximum des informations**			
			1	2	3	4
Niveau d'habilitation minimum des utilisateurs	0	1				
		2				
		3	F-C2	F-C2	F-B1	F-B3
	1	1	N			
		2	F-C2			
		3	F-C2	F-C2	F-B1	F-B3
	2	1	N	N		
		2	F-C2	F-C2		
		3	F-C2	F-C2	F-B1	F-B2
	3	1	N	N	N	
		2	F-C2	F-C2	F-C2	
		3	F-C2	F-C2	F-B1	F-B2
	4	1	N	N	N	F-C2
		2	F-C2	F-C2	F-C2	F-C2
		3	F-C2	F-C2	F-B1	F-B1

Intégrité	**Mode d'exploitation** ↘		**Classification maximum des informations**			
			1	2	3	4
Niveau d'habilitation minimum des utilisateurs	0	1				
		2				
		3	F-IN	F-IN	F-J1	F-J3
	1	1	N			
		2	F-IN			
		3	F-IN	F-IN	F-J1	F-J2
	2	1	N	N		
		2	F-IN	F-IN		
		3	F-IN	F-IN	F-J1	F-J2
	3	1	N	N	N	
		2	F-IN	F-IN	F-IN	
		3	F-IN	F-IN	F-J1	F-J2
	4	1	N	N	N	F-IN
		2	F-IN	F-IN	F-IN	F-IN
		3	F-IN	F-IN	F-J1	F-J1

Objectifs minimum de sécurité :

F-C2	I/A	IDENTIFICATION / AUTHENTIFICATION
		La TOE doit identifier et authentifier de façon unique les utilisateurs.
		L'identification et l'authentification doivent avoir lieu avant toute interaction entre la TOE et l'utilisateur.
		D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies.
		Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles par des utilisateurs autorisés.
		Pour chaque interaction, la TOE doit pouvoir établir l'identité de l'utilisateur.
F-IN	I/A	IDENTIFICATION / AUTHENTIFICATION
		La TOE doit identifier et authentifier de façon unique les utilisateurs.
		L'identification et l'authentification doivent avoir lieu avant toute interaction entre la TOE et l'utilisateur.
		D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies.
		Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles pour consultation ou modification par des utilisateurs autorisés.
		Pour chaque interaction, la TOE doit pouvoir établir l'identité de l'utilisateur.

F-C2	CTL	CONTRÔLE D'ACCES
		La TOE doit pouvoir distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur individuel, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux.
		Il doit être possible de refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet.
		Il doit être également possible de limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas cet objet.
		Il doit être possible d'accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel.

		Il ne doit pas être possible à quelqu'un qui n'est pas un utilisateur autorisé d'accorder ou de retirer des droits d'accès à un objet.
		L'administration des droits doit disposer de contrôles pour limiter la propagation des droits d'accès.
		De même, seuls les utilisateurs autorisés doivent pouvoir introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.
		Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande.
		Les tentatives d'accès non autorisé doivent être rejetées.
F-Q2	CTL	CONTROLE D'ACCES
		La TOE doit pouvoir distinguer et administrer les droits d'accès des utilisateurs, des rôles et des processus aux objets désignés explicitement (le terme rôle désigne des utilisateurs qui ont des attributs spéciaux).
		Il doit être possible de restreindre l'accès des utilisateurs à ces objets d'une façon telle que cet accès ne soit possible que par l'intermédiaire de processus établis spécialement.
		Il doit être possible d'affecter des objets à un type prédéfini.
		Il doit être possible de spécifier pour chaque type d'objet, quels sont les utilisateurs, les rôles ou les processus qui peuvent disposer de certains types d'accès à ces objets.
		Limiter l'accès des utilisateurs aux objets d'un certain type d'une façon telle que cet accès ne soit possible que par l'intermédiaire de processus définis et fixés.
		Il ne devrait possible qu'aux utilisateurs autorisés de définir des types nouveaux, d'accorder ou de retirer des droits d'accès à des types.
		Ces actions doivent être initialisées explicitement par ces utilisateurs.
		Pour ces actions, toute communication entre l'utilisateur et la TOE doit se faire à travers un chemin de confiance.
		Les droits d'accès minimum suivants doivent exister : exécution, suppression, renommage (pour les objets exécutables), création d'objets d'un certain type, suppression d'objets d'un certain type.
		Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande.

		Les tentatives d'accès non autorisé doivent être rejetées.
F-IN	CTL	CONTRÔLE D'ACCES
		La TOE doit pouvoir distinguer et administrer les droits d'accès des utilisateurs, des rôles et des processus aux objets désignés explicitement (le terme rôle désigne des utilisateurs qui ont des attributs spéciaux).
		Il doit être possible de restreindre l'accès des utilisateurs à ces objets d'une façon telle que cet accès ne soit possible que par l'intermédiaire de processus établis spécialement.
		Il doit être possible d'affecter des objets à un type prédéfini.
		Il doit aussi être possible de spécifier pour chaque type d'objet quels sont les utilisateurs, les rôles ou les processus qui peuvent disposer de certains types d'accès à ces objets. Cela devrait permettre de limiter l'accès des utilisateurs aux objets d'un certain type d'une façon telle que cet accès ne soit possible que par l'intermédiaire de processus définis et fixés.
		Seuls les utilisateurs autorisés pourraient définir des types nouveaux, accorder ou retirer des droits d'accès à des types.
		Ces actions doivent être initialisées explicitement par ces utilisateurs.
		Pour ces actions, toute communication entre l'utilisateur et la TOE doit se faire à travers un chemin de confiance.
		Les droits d'accès minimum suivants doivent exister : lecture, écriture, ajout, suppression, renommage (pour tous les objets), exécution, suppression, renommage (pour les objets exécutables), création d'objets d'un certain type, suppression d'objets d'un certain type.
		Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande.
		Les tentatives d'accès non autorisé doivent être rejetées.

F-C2	IMP	IMPUTABILITE
		La TOE doit comporter un composant d'imputation qui soit capable pour chacun des évènements suivants, d'enregistrer cet événement avec les données exigées : utilisation du mécanisme d'identification et d'authentification : données exigées : date ; heure ; identité fournie par l'utilisateur ; identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé (par exemple identificateur du terminal) ; réussite ou échec de la tentative. actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits : données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de la tentative d'accès ; réussite de la tentative. création ou suppression d'un objet soumis à l'administration des droits : données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de l'action. actions d'utilisateurs autorisés affectant la sécurité de la TOE : données exigées : date ; heure ; identité de l'utilisateur ; type de l'action ; nom de l'objet sur lequel porte l'action (de telles actions sont l'introduction ou la suppression (suspension) d'utilisateurs : l'introduction ou le retrait de supports de stockage ; le démarrage ou l'arrêt de la TOE) ; Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation.
		Il doit être possible de mettre sélectivement en œuvre l'imputation pour un ou plusieurs utilisateurs.
		Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés.
		Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.
F-Q2	IMP	IMPUTABILITE
		La TOE doit comporter un composant d'imputation qui soit capable pour chacun des évènements suivants, d'enregistrer cet événement avec les données exigées :

		a) utilisation du mécanisme d'identification et d'authentification : - données exigées : date ; heure ; identité fournie par l'utilisateur ; identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé (par exemple identificateur du terminal) ; réussite ou échec de la tentative ; autorisation de l'utilisateur. b) actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits : - données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de la tentative d'accès ; réussite ou échec de la tentative ; attribut de l'objet. c) création ou suppression d'un objet soumis à l'administration des droits : - données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de l'action ; attribut de l'objet. d) actions d'utilisateurs autorisés affectant la sécurité de la TOE : - données exigées : date ; heure ; identité de l'utilisateur ; type de l'action ; nom et attribut de l'objet sur lequel porte l'action (de telles actions sont l'introduction ou la suppression (suspension) d'utilisateurs : l'introduction ou le retrait de supports de stockage ; le démarrage ou l'arrêt de la TOE ; l'assignation d'un attribut ; la modification des attributs, des marques ou de la classification d'un canal). e) Définition ou suppression de types : - données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; nom du type. f) assignation d'un type à un objet : - données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; nom du type. g) attribution ou révocation de droits d'accès à un objet ou un type d'objet : - données exigées : date ; heure ; identité de l'utilisateur ; type de l'action ; type du droit d'accès ; nom du sujet ; nom de l'objet ou nom du type d'objet. Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation.

		Il doit être possible de mettre sélectivement en œuvre l'imputation pour un ou plusieurs utilisateurs.
		Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés.
		Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.
		La structure des enregistrements d'imputation doit être décrite de façon complète.

F-C2	AU	AUDIT
		Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés.
		Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

F-C2	REU	REUTILISATION D'OBJET
		Tous les objets de stockage rendus à la TOE doivent, avant d'être réutilisé par d'autres sujets, être traités d'une manière telle qu'aucune conclusion ne puisse être tirée concernant leur contenu précédent.

Exigences Fonctionnelles

N°	Confidentialité	Mesure(s) mise(s) en place	Méthode de recette	avis de la MOA
	IDENTIFICATION / AUTHENTIFICATION			
1	La TOE doit identifier et authentifier de façon unique les utilisateurs.	RADIUS	Authentification avec deux comptes minimum différents	
2	L'identification et l'authentification doivent avoir lieu avant toute interaction entre la TOE et l'utilisateur.	Protocole SSH RADIUS	test de modification sans authentification	
3	D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies.	Protocole SSH RADIUS	test de modification avec mauvaise authentification	
4	Les informations d'authentification doivent être stockées de façons telles qu'elles soient seulement accessibles par des utilisateurs autorisés.	ACTIVE DIRECTORY	Audit et validation par RSSI	
5	Pour chaque interaction, la TOE doit pouvoir établir l'identité de l'utilisateur.	Protocole SSH RADIUS	Authentification avec deux comptes minimum différents	
	CONTRÔLE D'ACCES			
6	La TOE doit pouvoir distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur individuel, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux.	RADIUS	Tests de différents profils	
7	Il doit être possible de refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet.	RADIUS	Tests d'accès avec profil non-autorisé	
8	Il doit être également possible de limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas cet objet.	RADIUS	Tests de lecture avec profil limité	

9	Il doit être possible d'accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel.	RADIUS	Test modification avec un compte particulier	
10	Il ne doit pas être possible à quelqu'un qui n'est pas un utilisateur autorisé d'accorder ou de retirer des droits d'accès à un objet.	RADIUS ACTIVE DIRECTORY	Audit et validation par RSSI	
11	L'administration des droits doit disposer de contrôles pour limiter la propagation des droits d'accès.	RADIUS ACTIVE DIRECTORY	Audit et validation par RSSI	
12	De même, seuls les utilisateurs autorisés doivent pouvoir introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.	RADIUSACTIVE DIRECTORY	Audit et validation par RSSI	
13	Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande.	RADIUS	Test d'accès et vérification	
14	Les tentatives d'accès non autorisé doivent être rejetées.	RADIUS	Tests d'accès avec profil non-autorisé	
IMPUTABILITE				
	La TOE doit comporter un composant d'imputation qui soit capable pour chacun des évènements suivants, d'enregistrer cet événement avec les données exigées :			
	utilisation du mécanisme d'identification et d'authentification :			
15	données exigées : date ; heure ; identité fournie par l'utilisateur ; identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé (par exemple identificateur du terminal) ; réussite ou échec de la tentative.	RSYSLOG	Consultation des journaux	
	actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits :			
16	données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de la tentative d'accès ; réussite de la tentative.	RSYSLOG	Consultation des journaux	
	création ou suppression d'un objet soumis à l'administration des droits :			
17	données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de l'action.	RSYSLOG	Consultation des journaux	

	actions d'utilisateurs autorisés affectant la sécurité de la TOE :			
18	données exigées : date ; heure ;identité de l'utilisateur ; type de l'action ; nom de l'objet sur lequel porte l'action (de telles actions sont l'introduction ou la suppression (suspension) d'utilisateurs : l'introduction ou le retrait de supports de stockage ; le démarrage ou l'arrêt de la TOE) ;	RSYSLOG	Consultation des journaux	
19	Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation.	MYSQL	Tests de consultation avec profil non-autorisé	
20	Il doit être possible de mettre sélectivement en œuvre l'imputation pour un ou plusieurs utilisateurs.	RSYSLOG	Test d'imputation d'action avec plusieurs profils différents	
21	Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés.	LOGANALYZER	Audit et validation par RSSI	
22	Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.	LOGANALYZER	Test d'imputation d'action avec plusieurs profils différents	
AUDIT				
23	Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés.	LOGANALYZER	Audit et validation par RSSI	
24	Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.	LOGANALYZER	Test d'imputation d'action avec plusieurs profils différents	
REUTILISATION D'OBJET				
25	Tous les objets de stockage rendus à la TOE doivent, avant d'être réutilisé par d'autres sujets, être traités d'une manière telle qu'aucune conclusion ne puisse être tirée concernant leur contenu précédent.	X (relatif à l'organisation et les procédures en vigueur)	Audit et validation par RSSI	

Disponibilité

CONTROLE D'ACCES				
26	La TOE doit pouvoir distinguer et administrer les droits d'accès des utilisateurs, des rôles et des processus aux objets désignés explicitement (le terme rôle désigne des utilisateurs qui ont des attributs spéciaux).	RADIUS	Tests des droits sur différents équipements	
27	Il doit être possible de restreindre l'accès des utilisateurs à ces objets d'une façon telle que cet accès ne soit possible que par l'intermédiaire de processus établis spécialement.	RADIUS	Audit et validation par RSSI	
28	Il doit être possible d'affecter des objets à un type prédéfini.	ACTIVE DIRECTORY	Audit et validation par RSSI	
29	Il doit être possible de spécifier pour chaque type d'objet, quels sont les utilisateurs, les rôles ou les processus qui peuvent disposer de certains types d'accès à ces objets.	RADIUS ACTIVE DIRECTORY	Tests de différents profils	
30	Limiter l'accès des utilisateurs aux objets d'un certain type d'une façon telle que cet accès ne soit possible que par l'intermédiaire de processus définis et fixés.	RADIUS	Audit et validation par RSSI	
31	Il ne devrait être possible qu'aux utilisateurs autorisés de définir des types nouveaux, d'accorder ou de retirer des droits d'accès à des types.	RADIUS	Test de création/modification à un profil non autorisé	
32	Ces actions doivent être initialisées explicitement par ces utilisateurs.	RADIUS	Audit et validation par RSSI	
33	Pour ces actions, toute communication entre l'utilisateur et la TOE doit se faire à travers un chemin de confiance.	SSH	Audit et validation par RSSI	
34	Les droits d'accès minimum suivants doivent exister : exécution, suppression, renommage (pour les objets exécutables), création d'objets d'un certain type, suppression d'objets d'un certain type.	EAR	Audit et validation par RSSI	
35	Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande.	RADIUS	Test d'accès et vérification	
36	Les tentatives d'accès non autorisé doivent être rejetées.	RADIUS	Tests d'accès avec profil non-autorisé	

IMPUTABILITE				
	La TOE doit comporter un composant d'imputation qui soit capable pour chacun des évènements suivants, d'enregistrer cet événement avec les données exigées :			
	a) utilisation du mécanisme d'identification et d'authentification :			
37	heure ; identité fournie par l'utilisateur ; identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé (par exemple identificateur du terminal) ; réussite ou échec de la tentative ; autorisation de l'utilisateur.	RSYSLOG	Consultation des journaux	
	b) actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits :			
38	- données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de la tentative d'accès ; réussite ou échec de la tentative ; attribut de l'objet.	RSYSLOG	Consultation des journaux	
	c) création ou suppression d'un objet soumis à l'administration des droits :			
39	- données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de l'action ; attribut de l'objet.	RSYSLOG	Consultation des journaux	
	d) actions d'utilisateurs autorisés affectant la sécurité de la TOE :			
40	- données exigées : date ; heure ;identité de l'utilisateur ; type de l'action ; nom et attribut de l'objet sur lequel porte l'action (de telles actions sont l'introduction ou la suppression (suspension) d'utilisateurs : l'introduction ou le retrait de supports de stockage ; le démarrage ou l'arrêt de la TOE ; l'assignation d'un attribut ; la modification des attributs, des marques ou de la classification d'un canal).	RSYSLOG	Consultation des journaux	
	e) Définition ou suppression de types :			
41	- données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; nom du type.	RSYSLOG	Consultation des journaux	

	f) assignation d'un type à un objet :			
42	- données exigées : date ; heure ; identité de l'utilisateur ; nom de l'objet ; nom du type.	RSYSLOG	Consultation des journaux	
	g) attribution ou révocation de droits d'accès à un objet ou un type d'objet :			
43	- données exigées : date ; heure ; identité de l'utilisateur ; type de l'action ; type du droit d'accès ; nom du sujet ; nom de l'objet ou nom du type d'objet.	RSYSLOG	Consultation des journaux	
44	Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation.	MYSQL	Tests de consultation avec profil non-autorisé	
45	Il doit être possible de mettre sélectivement en œuvre l'imputation pour un ou plusieurs utilisateurs.	RSYSLOG	Test d'imputation d'action avec plusieurs profils différents	
46	Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés.	LOGANALYZER	Audit et validation par RSSI	
47	Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.	LOGANALYZER	Test d'imputation d'action avec plusieurs profils différents	
48	La structure des enregistrements d'imputation doit être décrite de façon complète.	MYSQL	Audit et validation par RSSI	

Intégrité

IDENTIFICATION / AUTHENTIFICATION				
49	La TOE doit identifier et authentifier de façon unique les utilisateurs.	RADIUS	Authentification avec deux comptes minimum différents	
50	L'identification et l'authentification doivent avoir lieu avant toute interaction entre la TOE et l'utilisateur.	Protocole SSH RADIUS	test de modification sans authentification	
51	D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies.	Protocole SSHRADIUS	test de modification avec mauvaise authentification	

52	Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles pour consultation ou modification par des utilisateurs autorisés.	ACTIVE DIRECTORY	Audit et validation par RSSI	
53	Pour chaque interaction, la TOE doit pouvoir établir l'identité de l'utilisateur.	Protocole SSH RADIUS	Authentification avec deux comptes minimum différents	
CONTRÔLE D'ACCES				
54	La TOE doit pouvoir distinguer et administrer les droits d'accès des utilisateurs, des rôles et des processus aux objets désignés explicitement (le terme rôle désigne des utilisateurs qui ont des attributs spéciaux).	RADIUS	Tests des droits sur différents équipements	
55	Il doit être possible de restreindre l'accès des utilisateurs à ces objets d'une façon telle que cet accès ne soit possible que par l'intermédiaire de processus établis spécialement.	RADIUS	Audit et validation par RSSI	
56	Il doit être possible d'affecter des objets à un type prédéfini.	ACTIVE DIRECTORY	Audit et validation par RSSI	
57	Il doit aussi être possible de spécifier pour chaque type d'objet quels sont les utilisateurs, les rôles ou les processus qui peuvent disposer de certains types d'accès à ces objets. Cela devrait permettre de limiter l'accès des utilisateurs aux objets d'un certain type d'une façon telle que cet accès ne soit possible que par l'intermédiaire de processus définis et fixés.	RADIUS ACTIVE DIRECTORY	Tests de différents profils	
58	Seuls les utilisateurs autorisés pourraient définir des types nouveaux, accorder ou retirer des droits d'accès à des types.	RADIUS	Test de création/modification à un profil non autorisé	
59	Ces actions doivent être initialisées explicitement par ces utilisateurs.	RADIUS	Audit et validation par RSSI	
60	Pour ces actions, toute communication entre l'utilisateur et la TOE doit se faire à travers un chemin de confiance.	SSH	Audit et validation par RSSI	

61	Les droits d'accès minimum suivants doivent exister : lecture, écriture, ajout, suppression, renommage (pour tous les objets), exécution, suppression, renommage (pour les objets exécutables), création d'objets d'un certain type, suppression d'objets d'un certain type.	EAR	Test des différents droits	
62	Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande.	RADIUS	Test d'accès et vérification	
63	Les tentatives d'accès non autorisé doivent être rejetées.	RADIUS	Tests d'accès avec profil non-autorisé	
64	La toe doit pouvoir être accessible localement même en cas de défaillance réseau.	EAR	Test d'accès sans réseau disponible	

Exigences Non Fonctionnelles

ORGANISATIONNELLES				
65	La solution doit permettre de réduire de min 66% le temps consacré aux changements des mots de passe	Relatif à l'ensemble de la solution	Audit et validation par Contrôle de gestion	
66	La solution doit permettre à un groupe d'utilisateur restreint (max 20 pax) de mettre en œuvre la PSSI en vigueur	Relatif à l'ensemble de la solution	Audit et validation par Contrôle de gestion	
TECHNIQUES				
67	La solution doit être compatible avec min 85% du parc d'équipements actifs	RADIUS SSH	Audit et validation par équipe DEX/RZO	

Contraintes

ORGANISATIONNELLES				
68	Les personnels peuvent avoir une formation interne, mais ne doivent pas avoir de formation extérieure pour manager la solution	Relatif à l'organisation interne	Audit et validation par Contrôle de gestion	
69	Les ressources en personnel pour le projet sont de 1 personne 3jours par semaine.	Relatif à l'organisation interne	Audit et validation par Contrôle de gestion	
70	La TOE doit respecter la PSSI en vigueur	Relatif aux procédures internes	Audit et validation par RSSI	
TECHNIQUES				
71	La solution doit s'appuyer sur l'Active Directory en place pour authentifier les utilisateurs	ACTIVE RIRECTORY	Authentification avec compte AD	
72	L'ergonomie de l'interface d'administration de la solution doit être une GUI ou une WebUI. Une CLI est jugée trop complexe par le client.	RADIUS ACTIVE DIRECTORY LOGANALYZER	Audit et validation par équipe DEX/RZO	
73	La solution doit s'intégrer dans l'architecture actuelle. (SHEM / virtualisation sur ESX)	RADIUS (NPS) CENTOS	Audit et validation par équipe hébergement	
74	La solution ne doit pas modifier la configuration des postes client d'administration	SSH	Audit et validation par équipe DIC	
FINANCIERES				
75	La solution ne doit pas engendrer de coûts supplémentaires à ceux déjà engagés	SERVEUR DE JOURNALISATION RADIUS NPS	Audit et validation par Contrôle de gestion	

ANNEXE C : INSTALLATION DU SERVEUR DE JOURNALISATION

Le serveur CENTOS 6 a été partitionné tel quel :

HDD :
SDA1 : 200Mo /boot
SDA2 : 343863Mo /var
SDA3 : 10240Mo /
SDA4 : 4096Mo SWAP

Installation minimale

Configuration des repository centos(DVD)

```
# vi /etc/yum.repos.d/CentOS-Media.repo

enable=1
```

Monter le DVD

```
# mkdir /media/cdrom
# mount -t iso9660 /dev/sr0 /media/cdrom/
```

Configuration Réseaux:

Modifier le fichier de configuration réseau :

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0

ONBOOT=yes
BOOTPROTO=static
```

Installation SSH2

Commande d'installation via dvd :

```
# yum --disablerepo=\* --enablerepo=c6-media install ssh2
```

Installation Apache

```
# yum --disablerepo=\* --enablerepo=c6-media install httpd
```

Installation de Mysql:

```
# yum --disablerepo=\* --enablerepo=c6-media install mysql
```

Installation de Mysql-server:

```
# yum --disablerepo=\* --enablerepo=c6-media install mysql-
server
```

Installation rsyslog-mysql

```
# yum --disablerepo=\* --enablerepo=c6-media install rsyslog-
mysql
```

Installation VIM

```
# yum --disablerepo=\* --enablerepo=c6-media install vim
```

Installation MAN

```
# yum --disablerepo=\* --enablerepo=c6-media install man
```

Installation PHP

```
# yum --disablerepo=\* --enablerepo=c6-media install php
```

Installation PHP-MYSQL

```
# yum --disablerepo=\* --enablerepo=c6-media install php-mysql
```

Configuration MYSQL:

```
# chkconfig mysqld on
#service mysqld start
```

Changement du mot de passe de root mysql :

```
# mysqladmin –u root password « nouveau mdp »
```

Username :root
Password : Clnpwd2Mysql

Username: user_loganalyzer
Password: Clnpwd210AnAly3er

Créer la base de données:

```
# cp /usr/share/doc/rsyslog-mysql-5.8.10/created.sql /opt
# mysql –u root –p < /opt/created.sql
```

```
#Mysql> GRANT ALL ON Syslog.* TO user_loganalyzer@localhost
IDENTIFIED BY "Clnpwd210gAnAly3er";
#Mysql> FLUSH PRIVILEGES;
```

Configuration de RSYSLOG

Sauvegarder le fichier de configuration

```
# cp /etc/rsyslog.conf /etc/rsyslog.conf.bkp
```

Modifier le fichier de configuration de rsyslog « rsyslog.conf »

```
# vi /etc/rsyslog.conf
```

```
$ModLoad imudp
$UDPServerRun 514

$ModLoad imtcp
$InputTCPServerRun 514

$EscapeControlCharactersOnReceive off
#$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
$RuleSet RSYSLOG_DefaultRuleset
```

```
*.* /var/log/messages
*.* :ommysql:localhost,Syslog,user_loganalyzer,Clnpwd210gAnAly3er

$ModLoad ommysql

$template dbFormat,"insert into SystemEvents (Message,
Facility,FromHost, Priority, DeviceReportedTime, ReceivedAt,
InfoUnitID, SysLogTag, EventLogType, EventSource, EventId,
EventUser) values ('%msg:F:10%', %syslogfacility%, '%HOSTNAME%',
%syslogpriority%, '%timereported:::date-mysql%',
'%timegenerated:::date-mysql%', %iut%, '%msg:F:3%', '%msg:F:6%',
'%msg:F:8%', '%msg:F:2%','%msg:F:4%')",sql

:syslogtag, contains, "Win" /var/log/windows #Personal checker,
don't need
& >localhost,Syslog, user_loganalyzer,Clnpwd210gAnAly3er;dbFormat
& ~ # DO NOT REMOVE OR DUPLICATE ENTRIES!
```

Relancer le service Rsyslog:

```
# service rsyslog restart
```

Configuration du firewall

```
# iptables –I INPUT 4 –p tcp --dport 80 –j ACCEPT
# iptables –I INPUT 5 –p tcp --dport 443 –j ACCEPT
# iptables –I INPUT 6 –p udp --dport 514 –j ACCEPT

# service iptables save
```

Configuration Service APACHE:

```
# chkconfig httpd on
#service httpd start
```

Permet le démarrage automatique du service

Sécurisation APACHE :

Editer le fichier de configuration d'apache pour modifier certains paramètres :

```
# vim /etc/httpd/conf/httpd.conf
```

Remplacer :

```
ServerSignature on
```

par :

```
ServerSignature off
```

et

```
ServerTokens OS
```

Par

```
ServerTokens Prod
```

Supprimer l'option `FollowSymLinks` partout où elle apparait

Remplacer l'option `Indexes` partout où elle apparait par `-Indexes`

Changer les droits des répertoires web :

```
# chown root /var/www/ -R
# chmod 755 /var/www/ -R
```

Sécurisation PHP :

Editer le fichier de configuration de PHP pour modifier certains paramètres :

```
# vim /etc/php.ini
```

Remplacer :

```
expose_php = On
```

par :

```
expose_php = Off
```

Création d'une page 404 :

Relancer les services web :

```
# /etc/init.d/httpd restart
```

Installation de loganalyzer

Copier l'archive de loganalyzer dans /opt

Extraire le contenu de l'archive dans

```
/var/www/html/
```

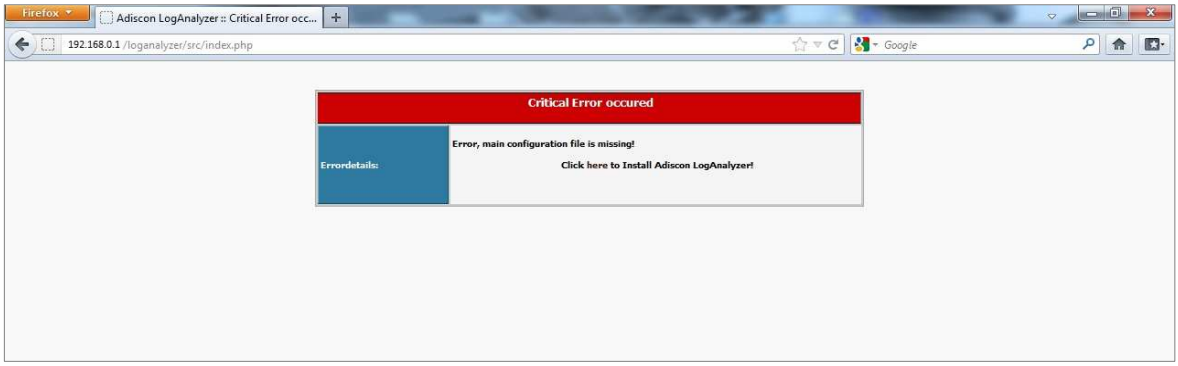
```
# tar -xvzf loganalyzer-3.6.3.tar.gz
```

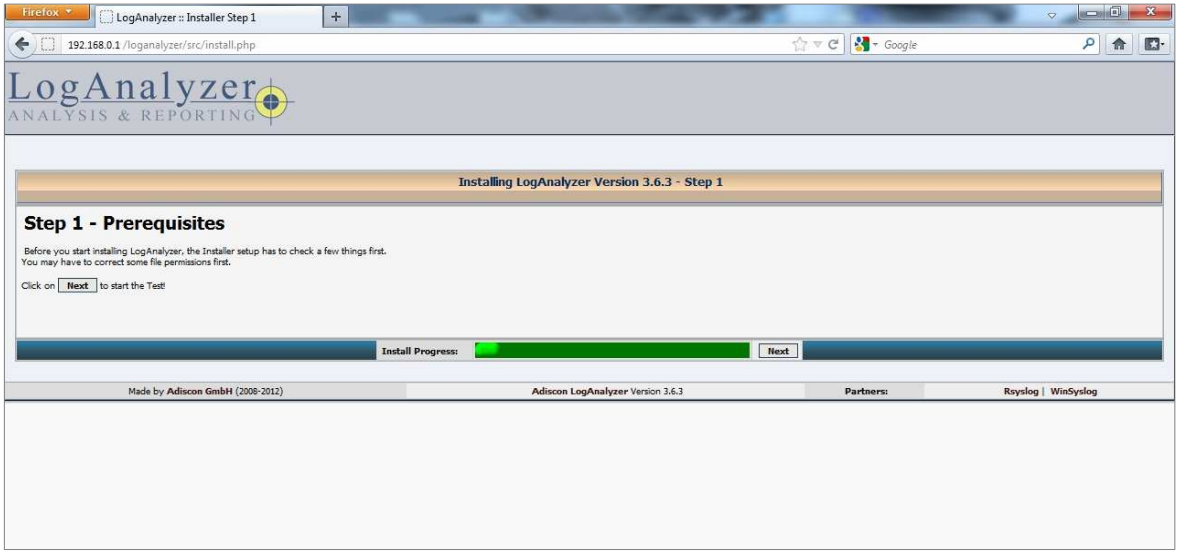
Renommer le répertoire nouvellement créé en « loganalyzer »

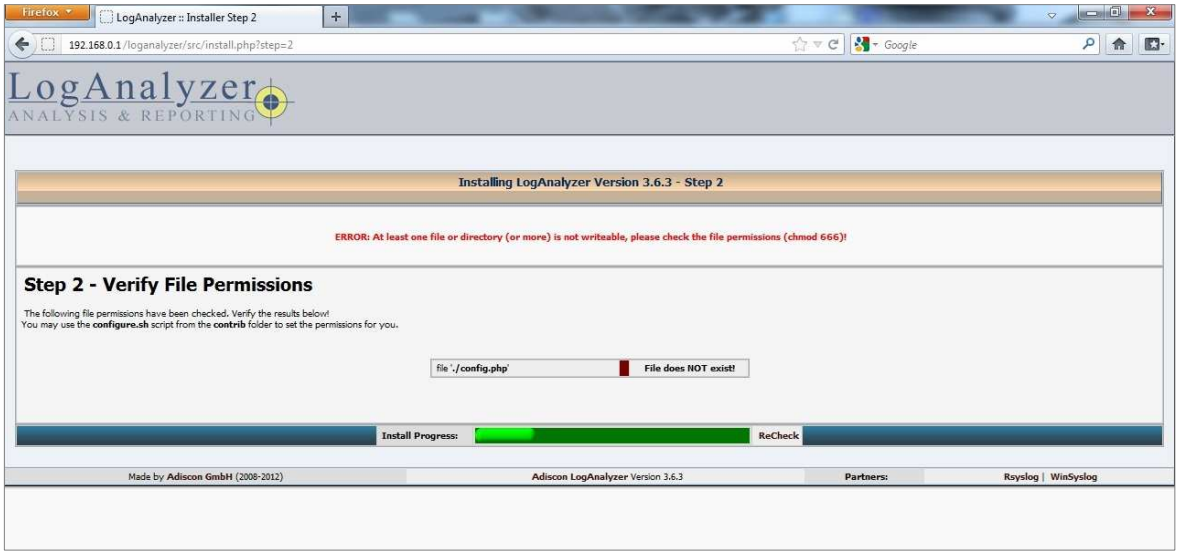
```
# mv -f loganalyzer-3.6.3/ loganalyzer
```

Dans un navigateur web, se connecter au script d'installation et suivre les étapes proposées pour l'installation :

http://@ip/loganalyzer/src/



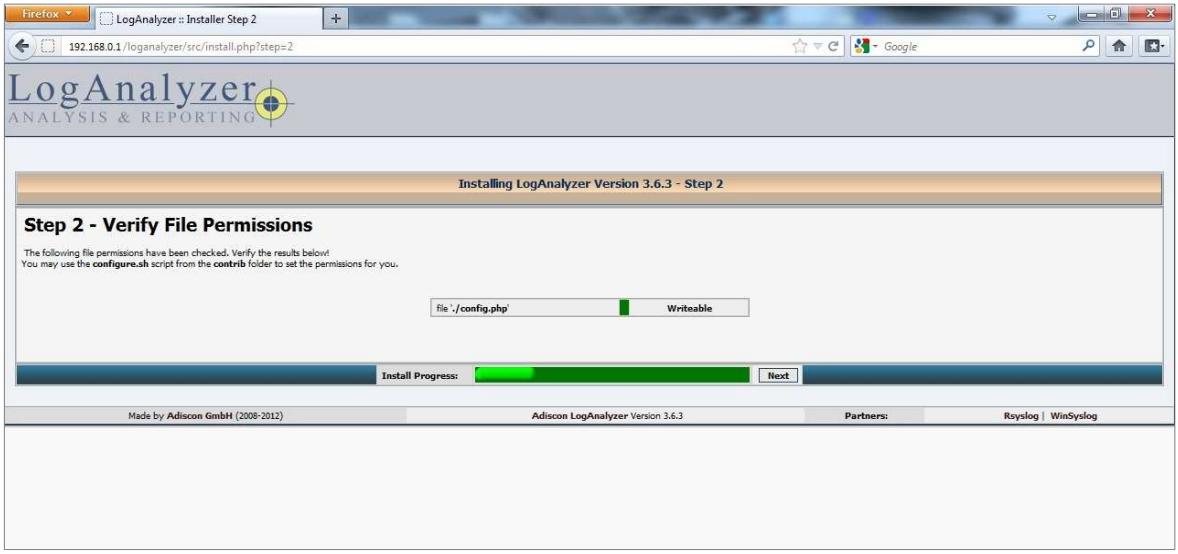


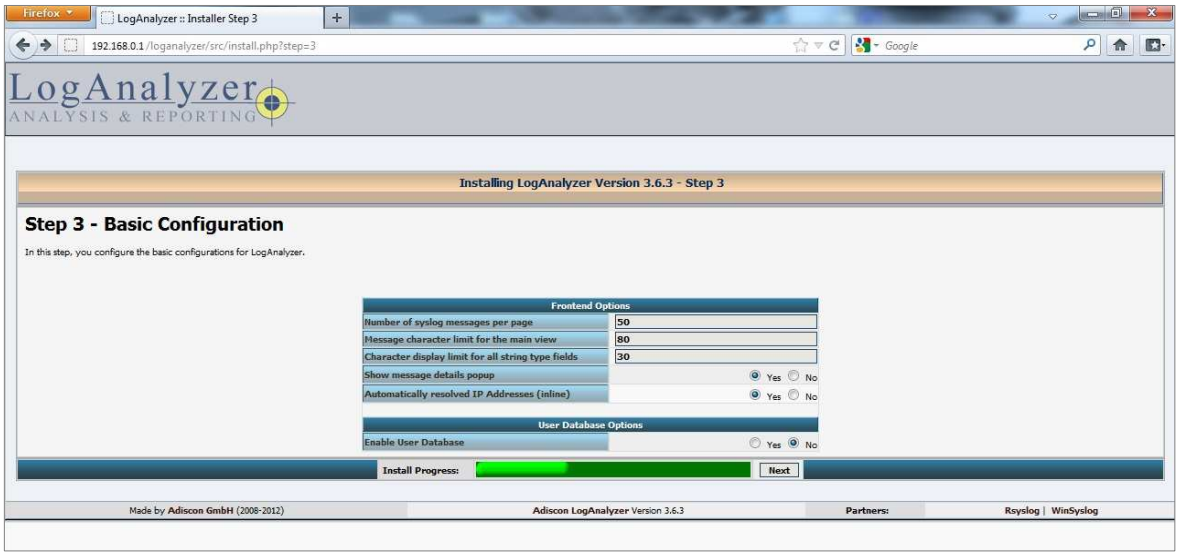


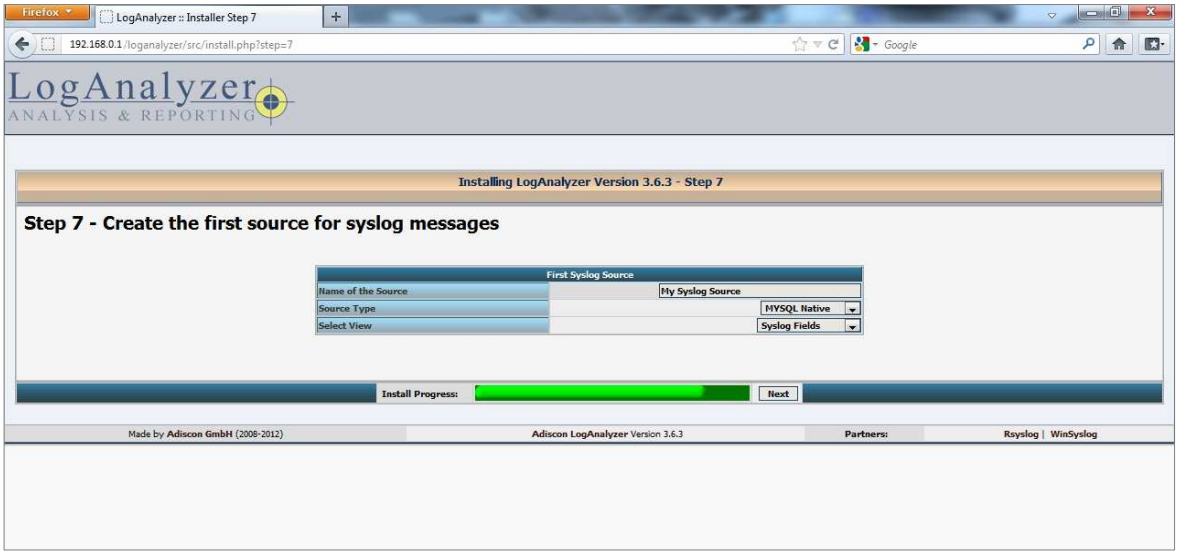
Un message indiquant que le fichier « config.php » n'existe pas apparait.
Le créer avec les droits adéquats en tapant les commandes suivantes :

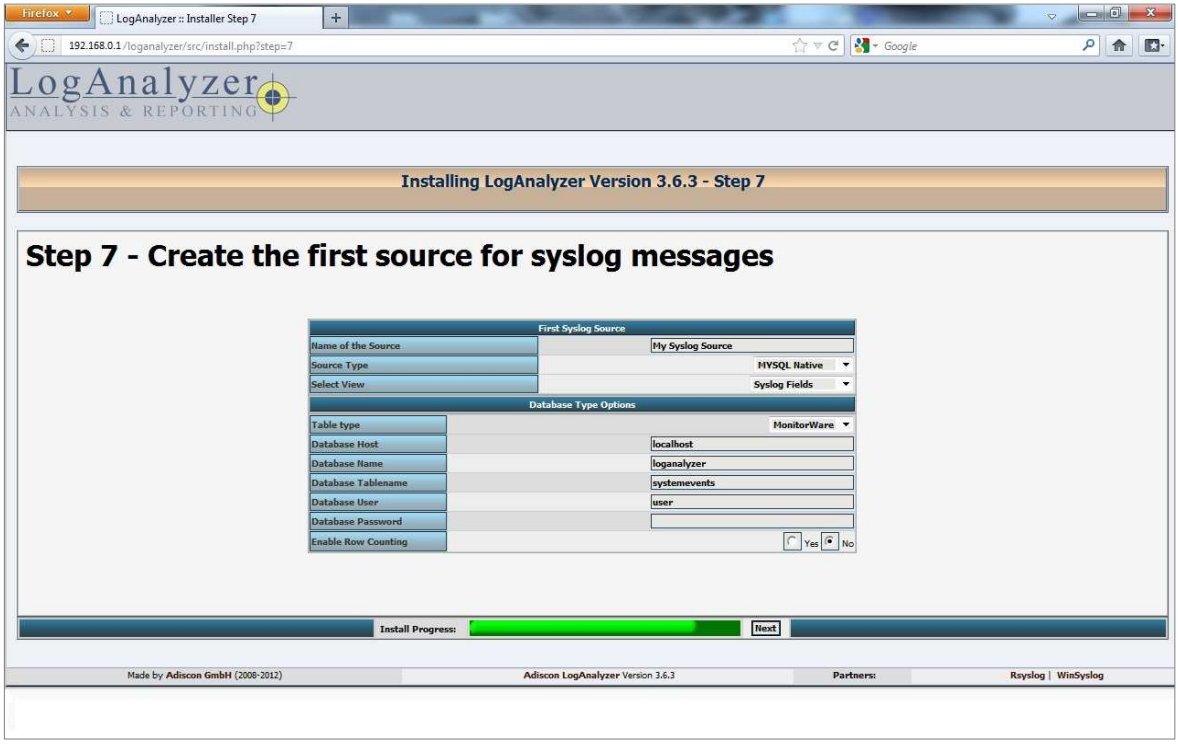
```
# touch /var/www/html/loganalyzer/src/config.php
# chmod 666 /var/www/html/loganalyzer/src/config.php
```

Continuer l'installation via l'interface web.


Firefox
LogAnalyzer :: Installer Step 2
192.168.0.1 /loganalyzer/src/install.php?step=2
LogAnalyzer
ANALYSIS & REPORTING
Installing LogAnalyzer Version 3.6.3 - Step 2
Step 2 - Verify File Permissions
The following file permissions have been checked. Verify the results below!
You may use the configure.sh script from the contrib folder to set the permissions for you.
file './config.php'
Writeable
Install Progress:
Next
Made by Adiscon GmbH (2008-2012)
Adiscon LogAnalyzer Version 3.6.3
Partners:
Rsyslog | WinSyslog


Firefox
LogAnalyzer :: Installer Step 3
192.168.0.1 /loganalyzer/src/install.php?step=3
LogAnalyzer
ANALYSIS & REPORTING
Installing LogAnalyzer Version 3.6.3 - Step 3
Step 3 - Basic Configuration
In this step, you configure the basic configurations for LogAnalyzer.
Frontend Options
Number of syslog messages per page
50
Message character limit for the main view
80
Character display limit for all string type fields
30
Show message details popup
Yes
No
Automatically resolved IP Addresses (inline)
Yes
No
User Database Options
Enable User Database
Yes
No
Install Progress:
Next
Made by Adiscon GmbH (2008-2012)
Adiscon LogAnalyzer Version 3.6.3
Partners:
Rsyslog | WinSyslog


Firefox
LogAnalyzer :: Installer Step 7
192.168.0.1 /loganalyzer/src/install.php?step=7
LogAnalyzer
ANALYSIS & REPORTING
Installing LogAnalyzer Version 3.6.3 - Step 7
Step 7 - Create the first source for syslog messages
First Syslog Source
Name of the Source
My Syslog Source
Source Type
MYSQL Native
Select View
Syslog Fields
Install Progress:
Next
Made by Adiscon GmbH (2008-2012)
Adiscon LogAnalyzer Version 3.6.3
Partners:
Rsyslog | WinSyslog



Correction bug loganalyzer :
Editer le fichier :

```
# Vim /var/www/html/loganalyzer/src/include/functions_common.php
```

Remplacer la ligne 1176:

```
        return htmlentities($myStr, ENT_NOQUOTES, "UTF-8");
```

par :

```
        return htmlentities($myStr, ENT_NOQUOTES, "CP1252");
```

La création des comptes de consultation est faite ultérieurement

ANNEXE D : COMPATIBILITE DES EQUIPEMENT AVEC LA SOLUTION

Constructeur	Modèle	compatible SSH/telnet	Authentification RADIUS	attribution droits d'administration	attribution droits restreint	Commentaire	Quantité	Totaux
3com	4210	oui	oui	oui	oui		81	551
	4400	oui	oui	oui	oui		200	
	4500	oui	oui	oui	oui		92	
	4800	oui	oui	oui	oui		22	
	3870	oui	non	X	X	limitation de la taille du mdp	3	
	5500	oui	oui	oui	oui		146	
	7900	oui	oui	oui	oui		5	
	4510	oui	oui	oui	oui		2	
HP	5500	oui	oui	oui	oui		17	86
	5120	oui	oui	oui	oui		34	
	3600	oui	oui	oui	oui		4	
	3100	oui	oui	oui	oui		31	
H3C	3600	oui	oui	oui	oui		6	45
	5500	oui	oui	oui	oui		12	
	5120	oui	oui	oui	oui		10	
	5800	oui	oui	oui	oui		3	
	3100	oui	oui	oui	oui		14	
ENTERASYS	A2	oui	oui	oui	oui		82	96
	C2	oui	oui	oui	oui		12	
	C3	oui	oui	oui	oui		1	
	N1	oui	oui	oui	oui	marche avec règle spécifique	1	
CISCO	3750	?	?	?	?		3	12
	2960	oui	oui	oui	oui		5	

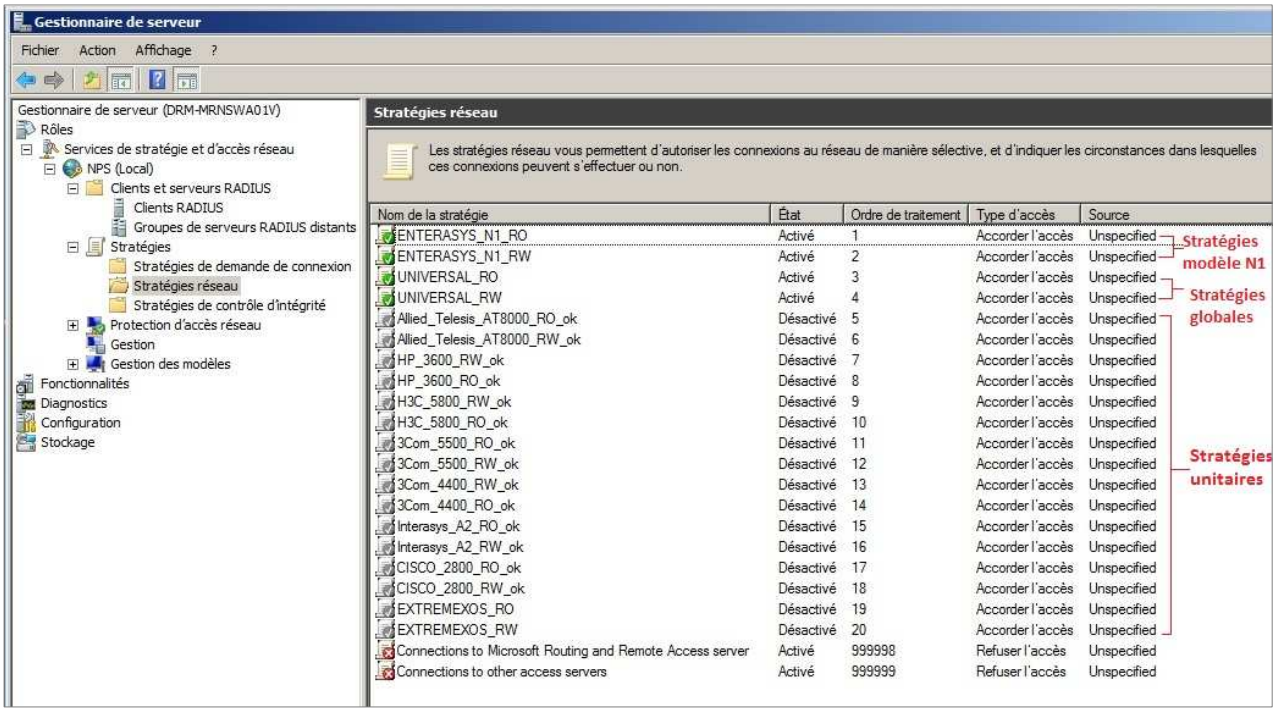
	2950	?	?	?	?	en panne (changement prévu)	1	
	2800	oui	oui	oui	oui		2	
	3620	telnet	oui	oui	oui	mettre firmware à jour	1	
Extreme Networks	summit200-24	oui	oui	oui	oui		1	**2**
	extreme X250	oui	oui	oui	oui		1	
Allied Telesis	8000	oui	oui	oui	oui		75	**136**
	8524	TELNET x	oui	oui	oui		10	
	8550	TELNET x	oui	oui	oui		4	
	8016	TELNET x	oui	oui	oui		1	
	8024	TELNET x	oui	oui	oui		18	
	8516	TELNET x	oui	oui	oui		3	
	9102	TELNET x	oui	oui	oui		2	
	AR 745	TELNET x	oui	oui	oui		1	
	8624	TELNET x	oui	oui	oui		6	
	9816	TELNET x	oui	oui	non		1	
	8324	?	non	non	non	Pas d'auth RADIUS implémentée	10	
	8350	?	non	non	non	Pas d'auth RADIUS implémentée	4	
	8326	?	?	?	?	en panne (changement prévu)	1	

	pleinement fonctionnel
	incompatibilité

total EARs	**928**
total fonctionnels	**862**
total incompatibles	**66**
ratio de compatibilité en %	**92,887931**

ANNEXE E : CONFIGURATION DES STRATEGIES DU SERVEUR NPS

Le résultat du travail de configuration du serveur NPS est le suivant :



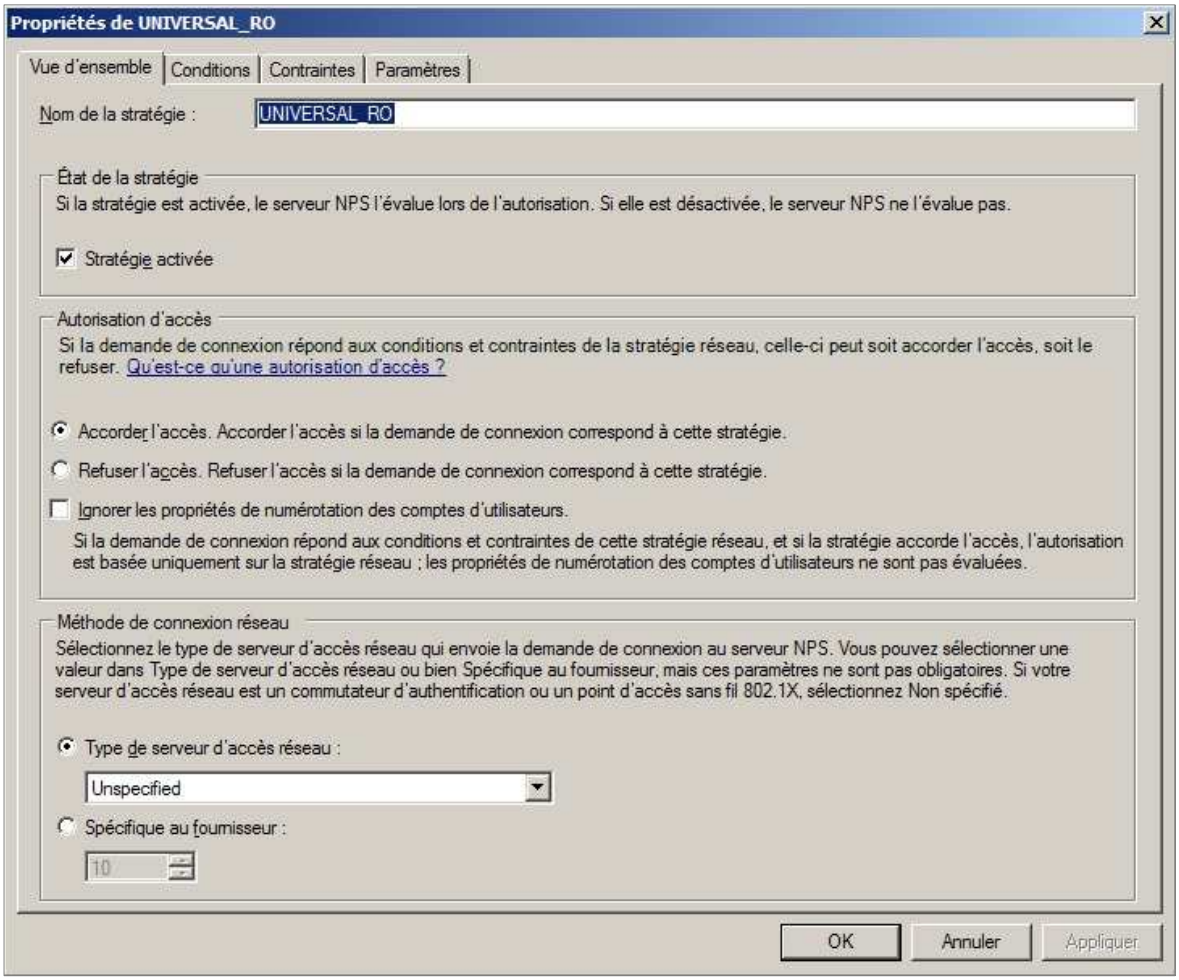
Comme le décrit le mode opératoire, plusieurs stratégies ont été configurées indépendamment (« Stratégies unitaires ») puis désactivées. Chaque paramétrage a été alors intégré à une stratégie (« Stratégies globales »). Seules les stratégies concernant le routeur ENTERASYS N1 ont été conservées pour compatibilité (« Stratégies modèle N1 »).

Ainsi on retrouve en premier lieu les stratégies activées concernant le routeur ENTERASYS N1 (1 = *droits de consultation* ; 2 = *droits d'administration*), puis les stratégies universelles traitant tous les autres matériels (3 = *droits de consultation* ; 4 = *droits d'administration*) et enfin l'ensemble des stratégies unitaires désactivées.

Le paramétrage des stratégies globales est le suivant :

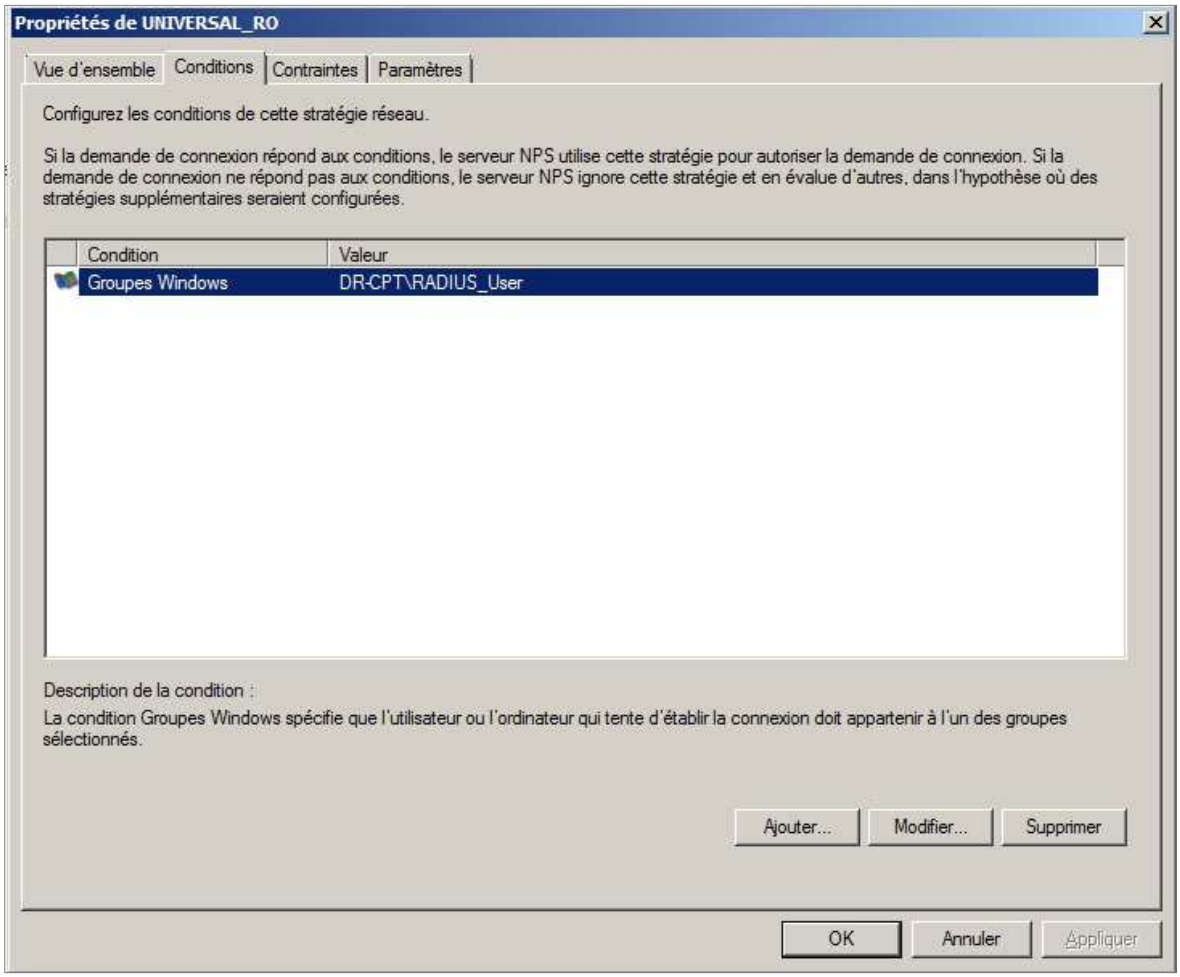
Droits de consultation :

Onglet :Vue d'ensemble :



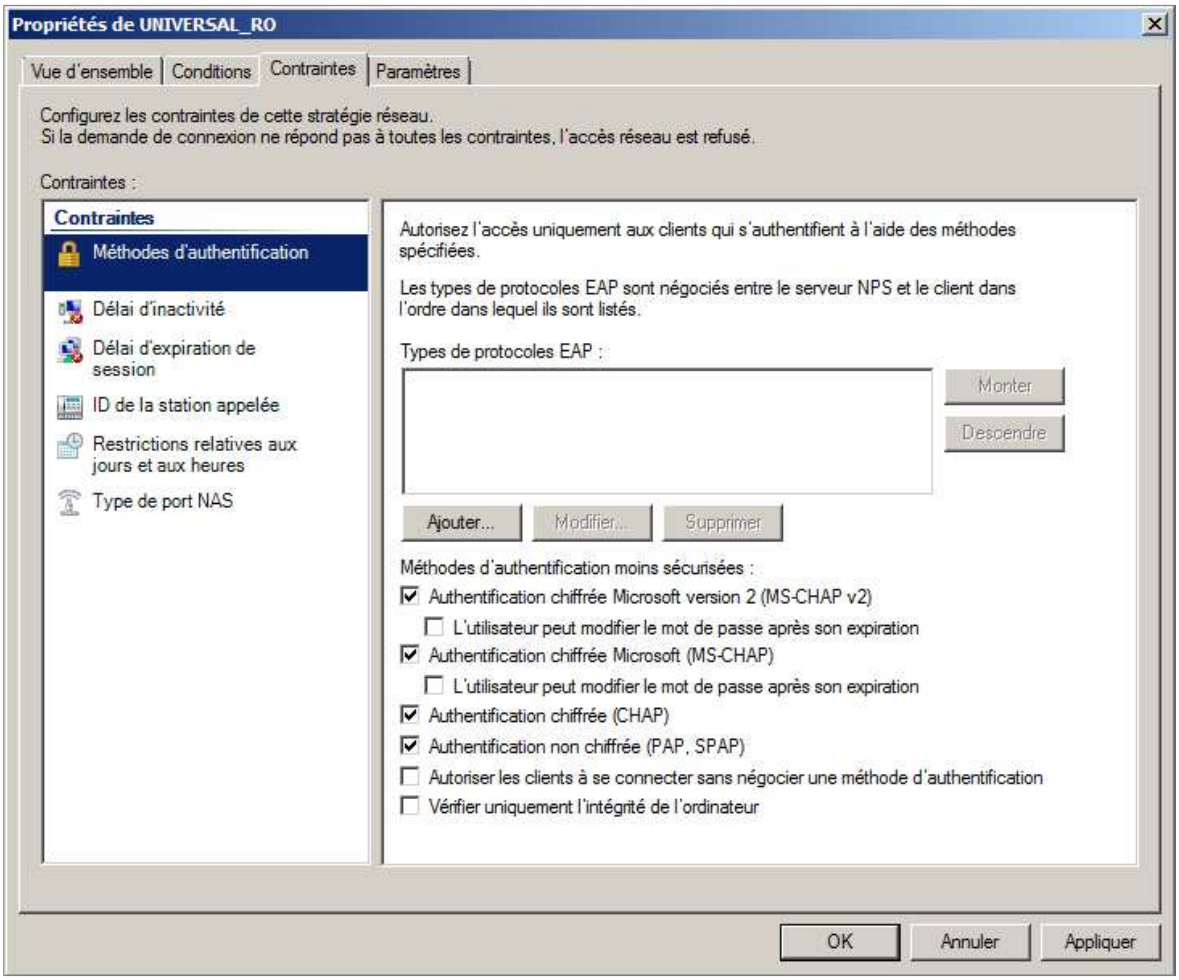
La stratégie doit être activée et Accorder l'accès.

Onglet :Conditions :



Définir le groupe d'utilisateur nécessitant seulement des droits de consultation.

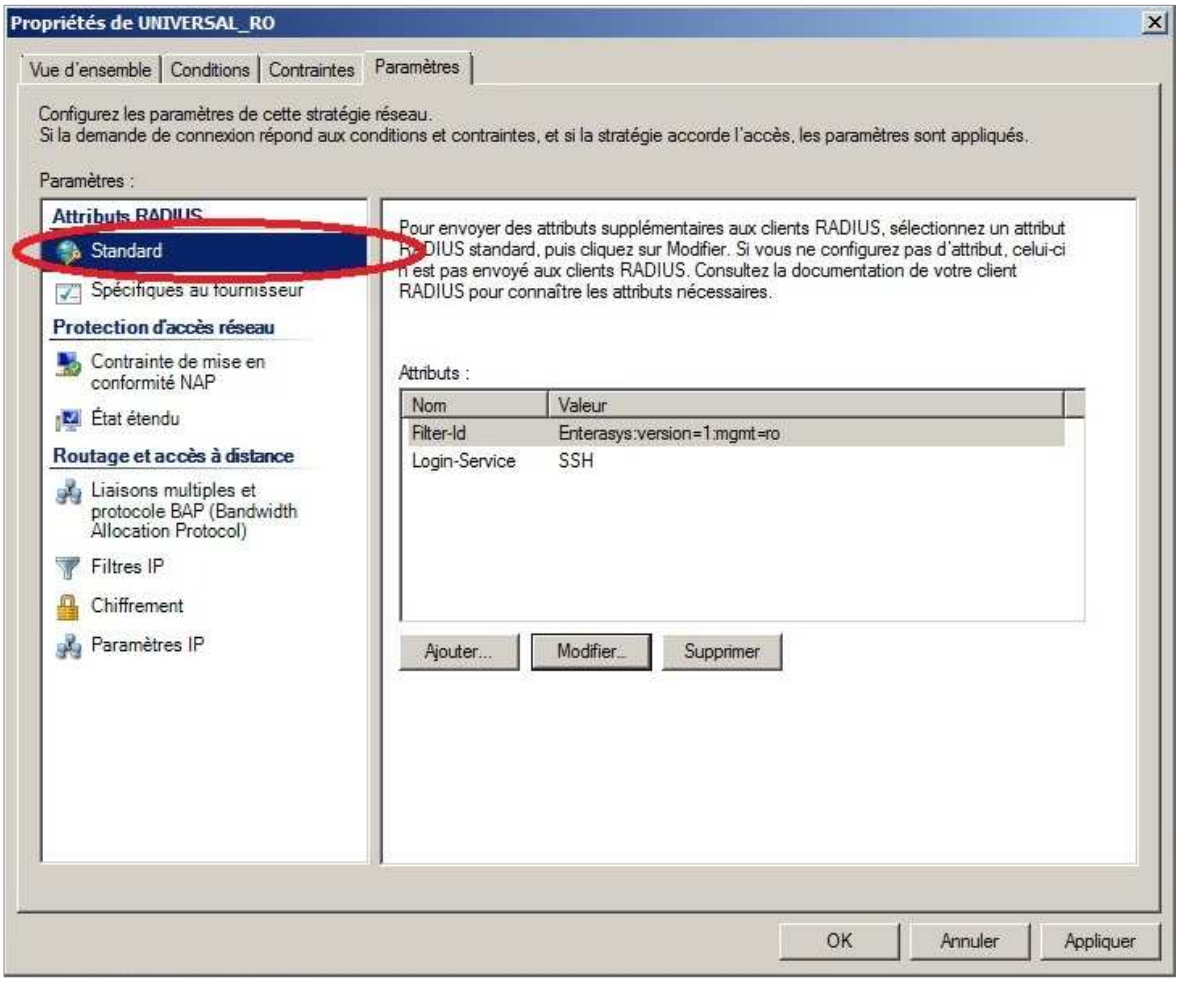
Onglet :Contraintes



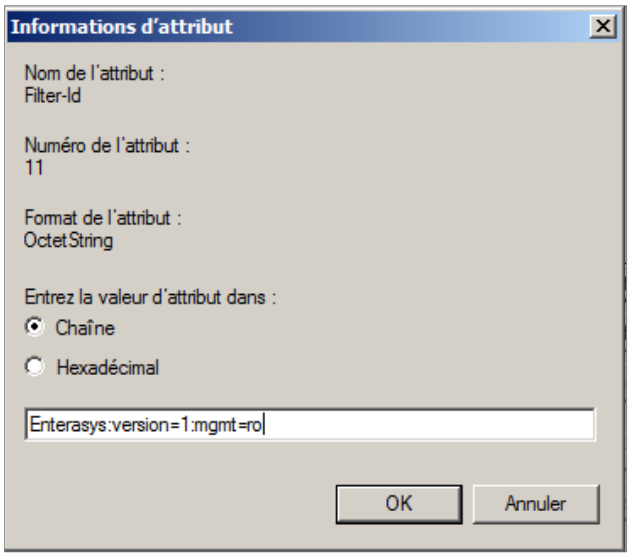
Sélectionner, en plus des modes présélectionnés, l'Authentification non chiffrée.

Onglet :Paramètres :

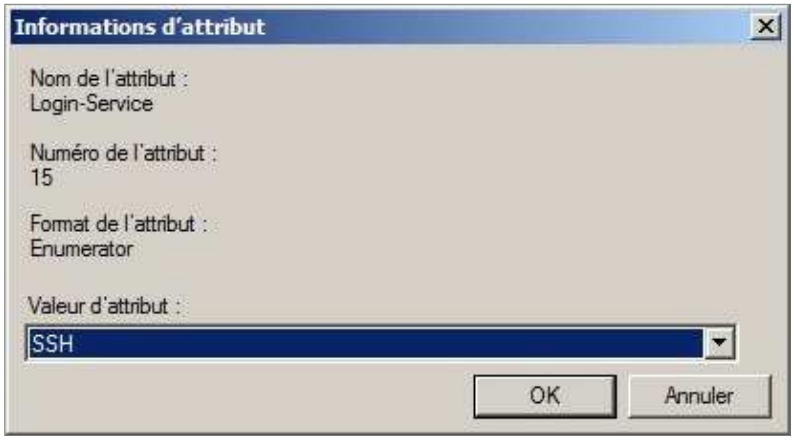
Pour les attributs standards :



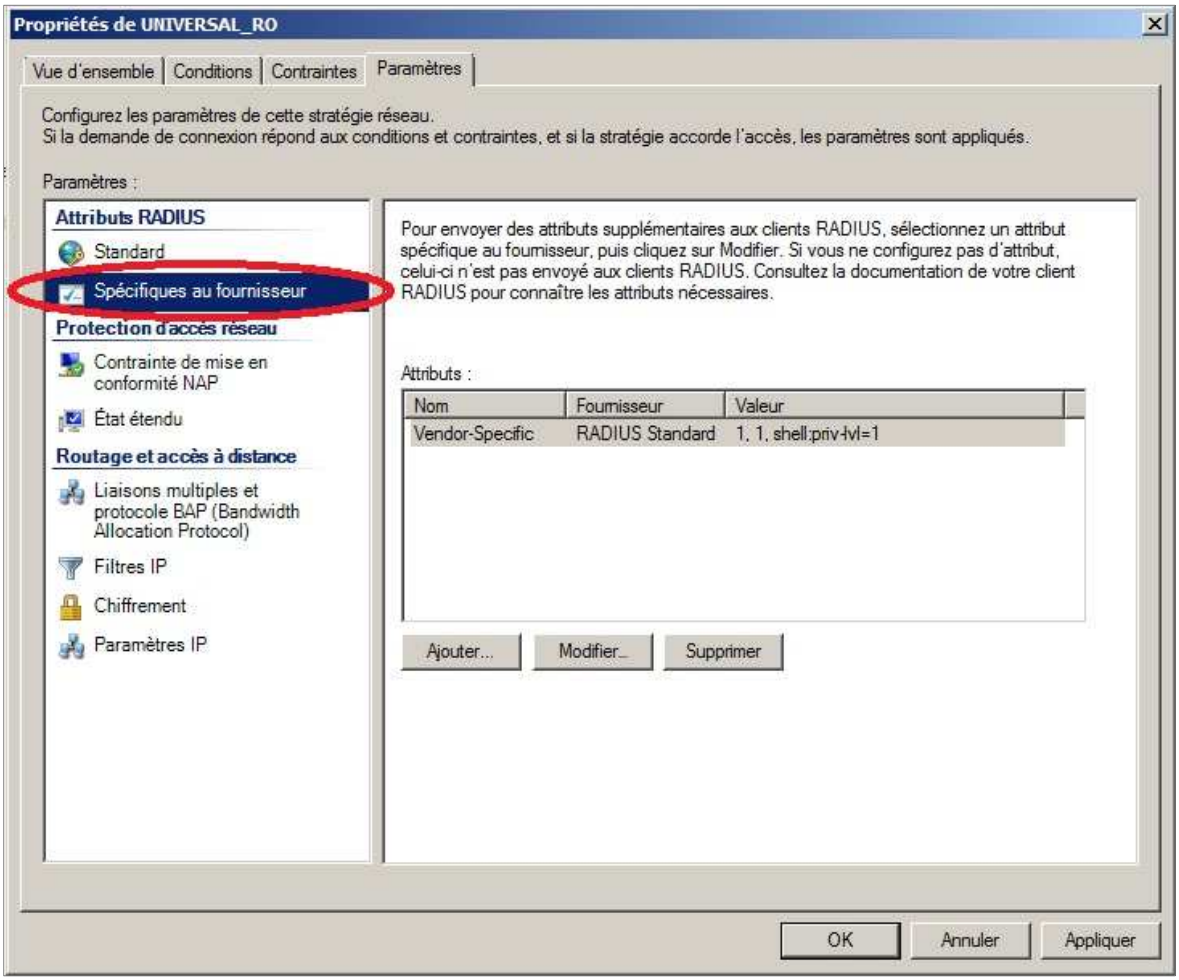
- Ajouter un attribut « Filter-Id » tel que :



- Ajouter un attribut « Login-Service » tel que :

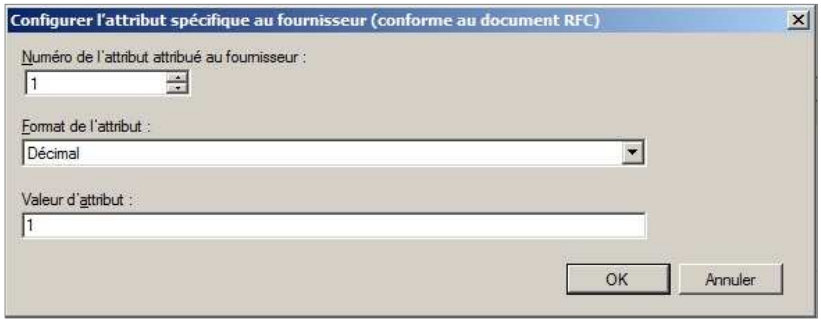


Pour les attributs Spécifiques au fournisseur :

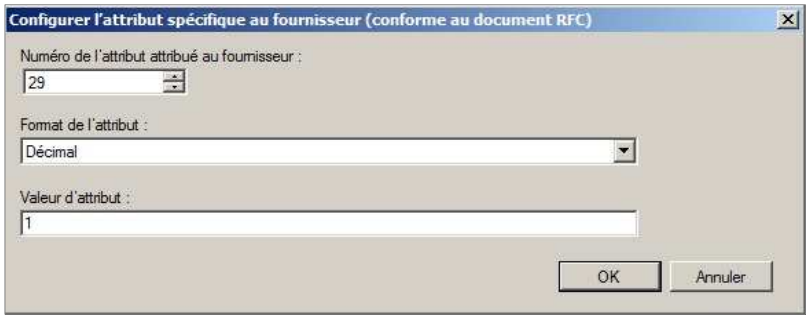


Ajouter trois attributs « Vendor-Specific » tels que :

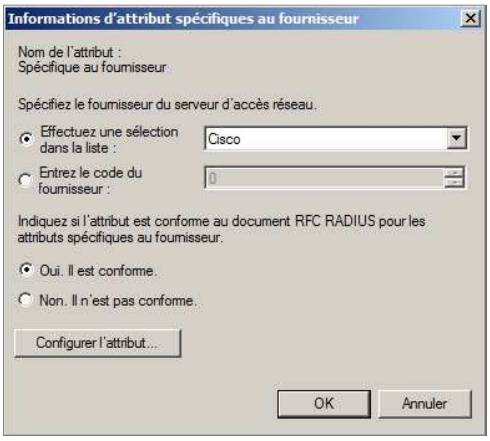
1)

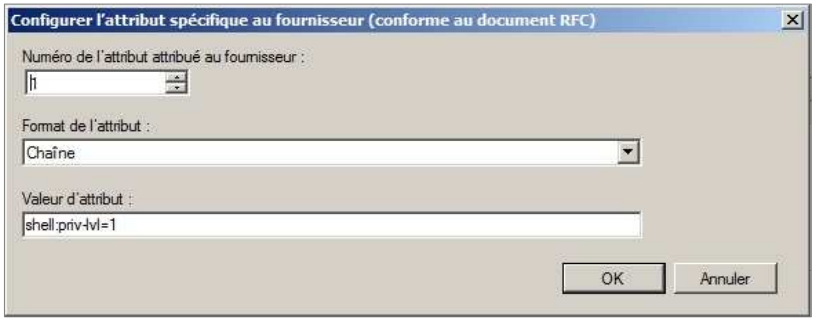


2)



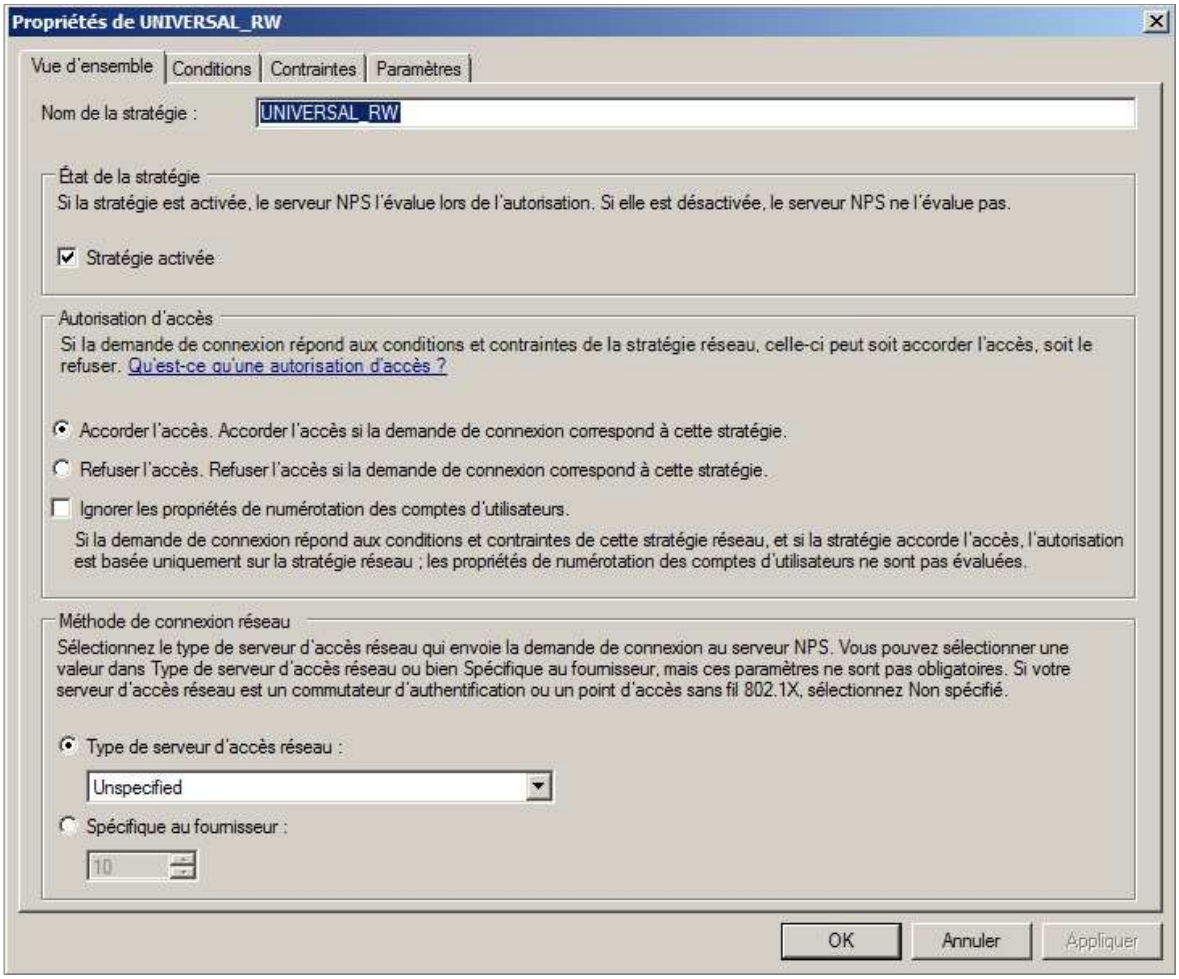
3)





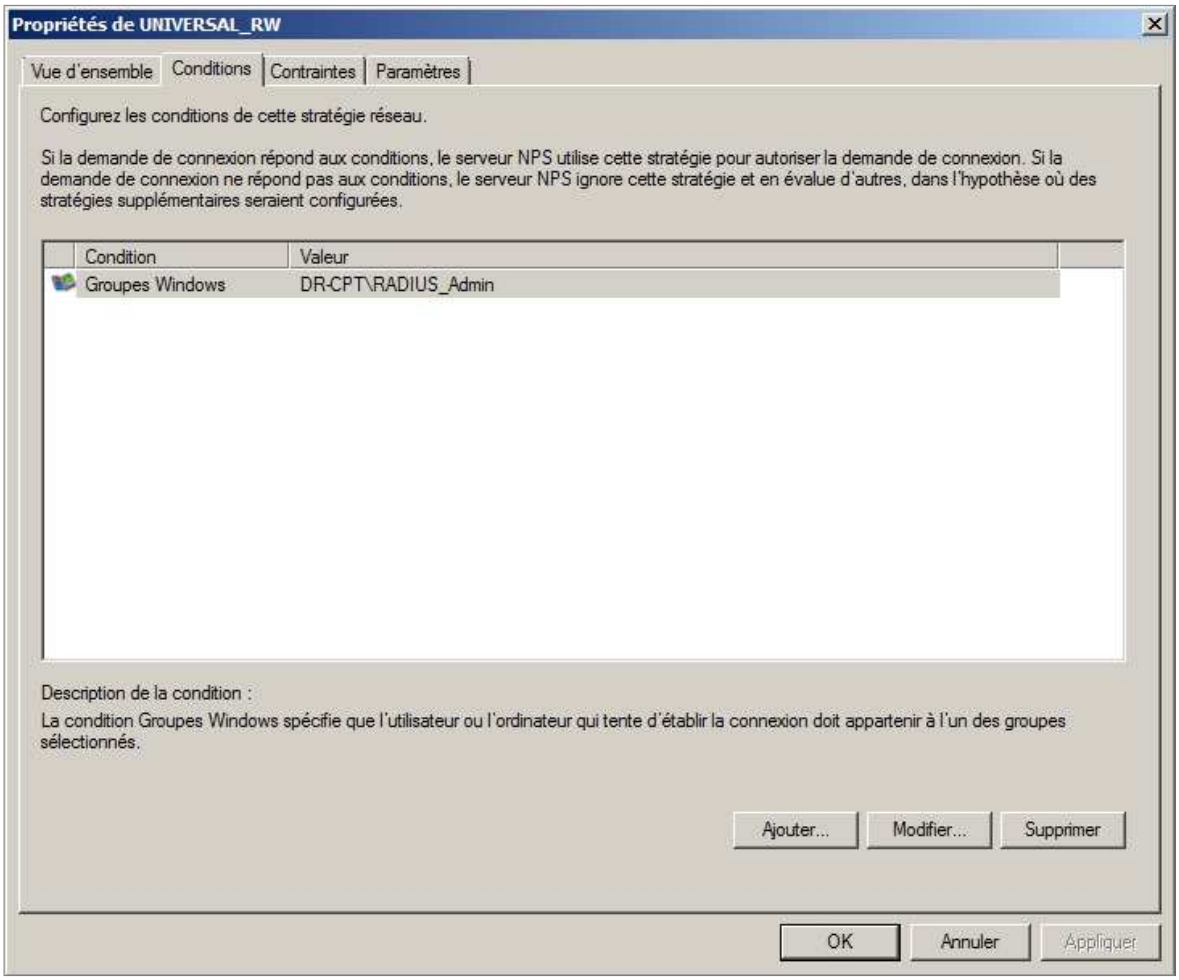
Droits d'administration :

Onglet :Vue d'ensemble :



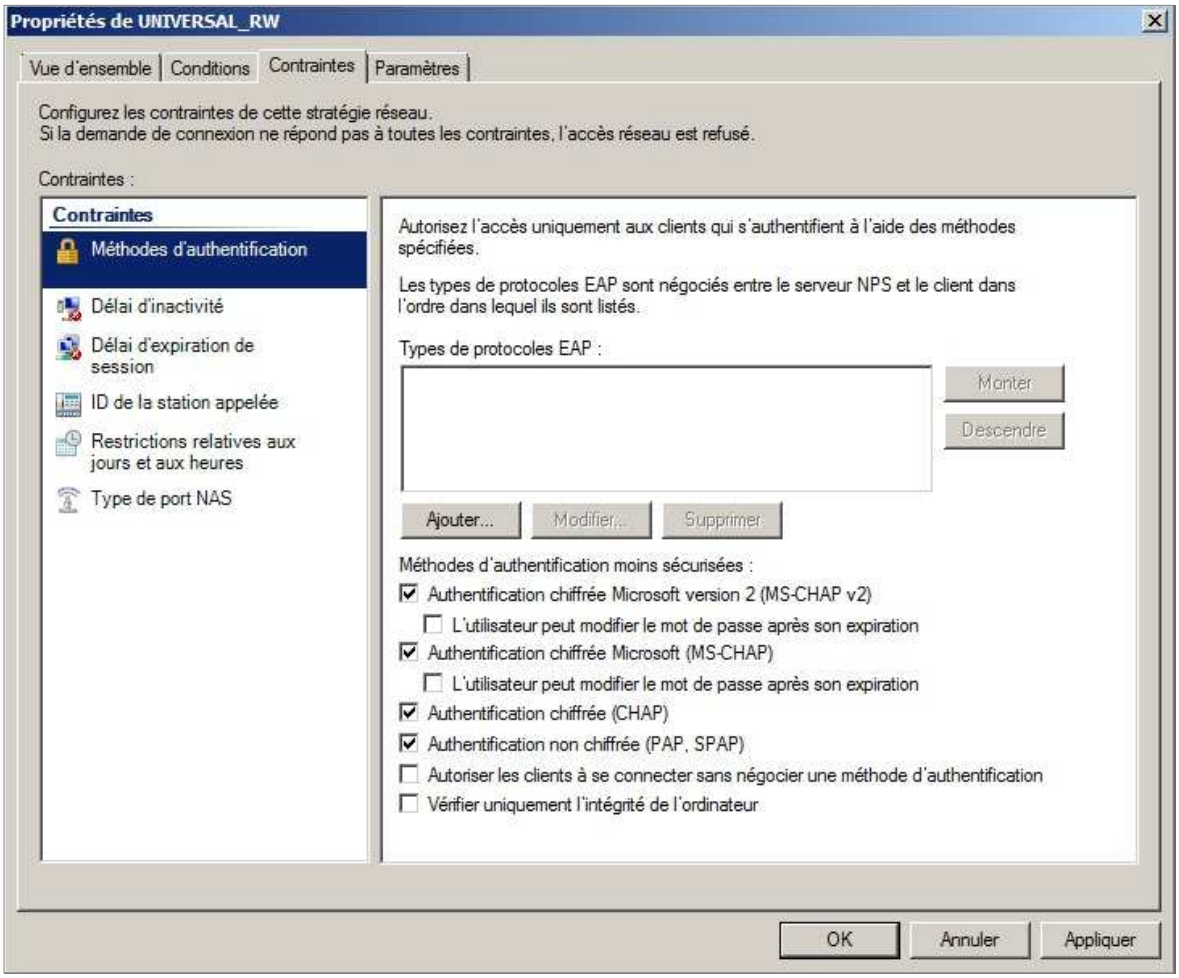
La stratégie doit être activée et Accorder l'accès.

Onglet :Conditions :



Définir le groupe d'utilisateur nécessitant des droits d'administration.

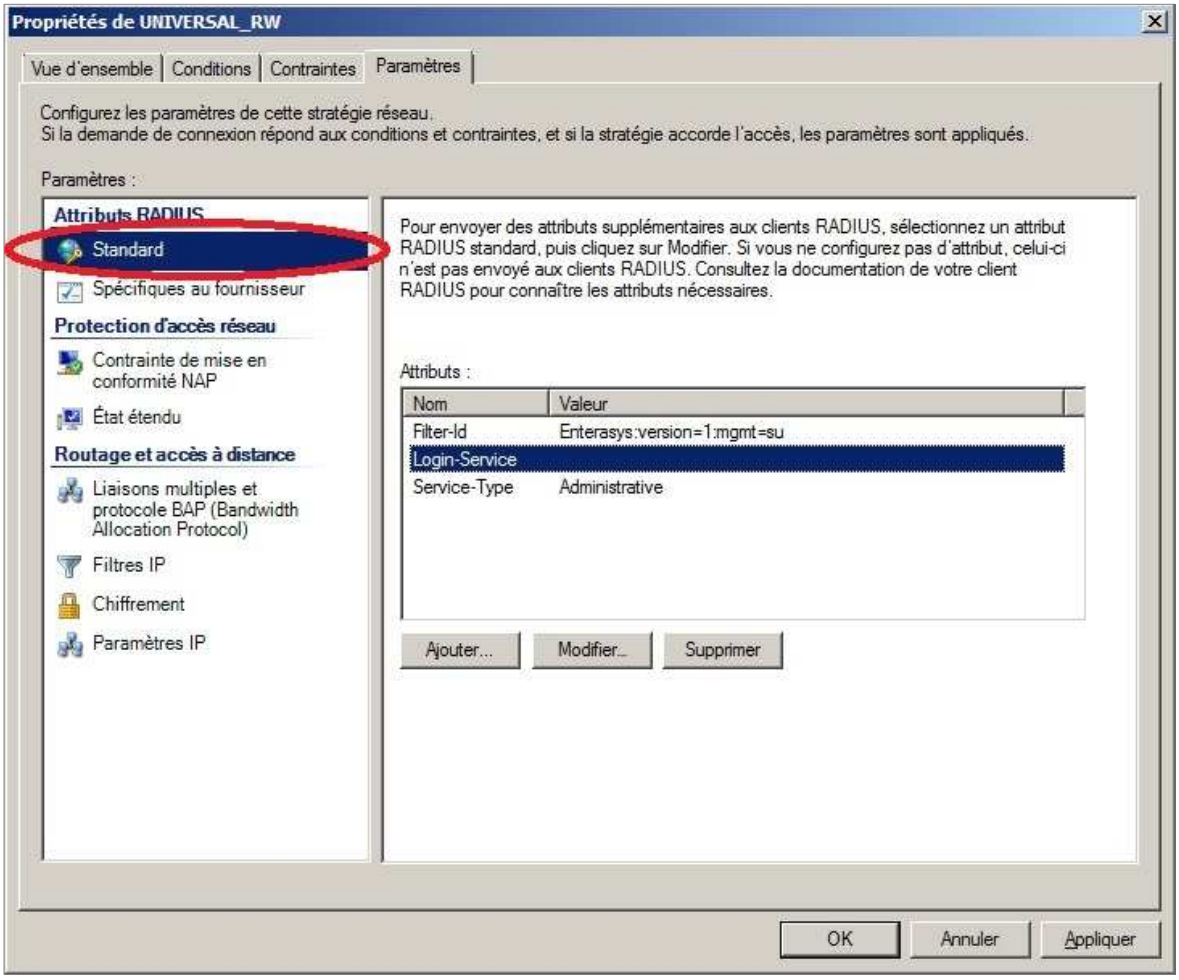
Onglet :Contraintes



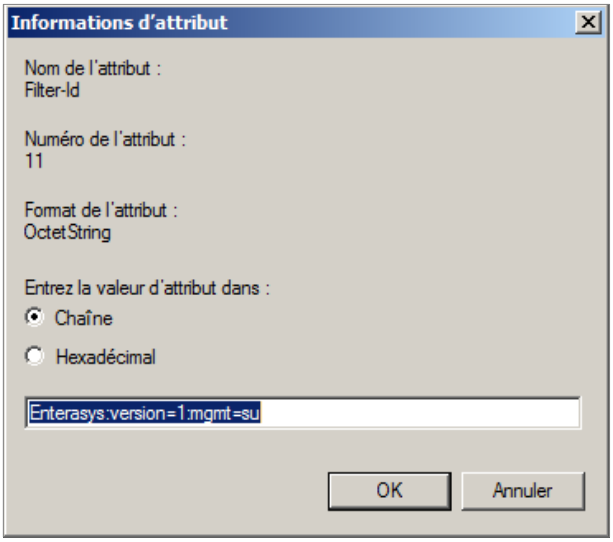
Sélectionner, en plus des modes présélectionnés, l'Authentification non chiffrée.

Onglet :Paramètres :

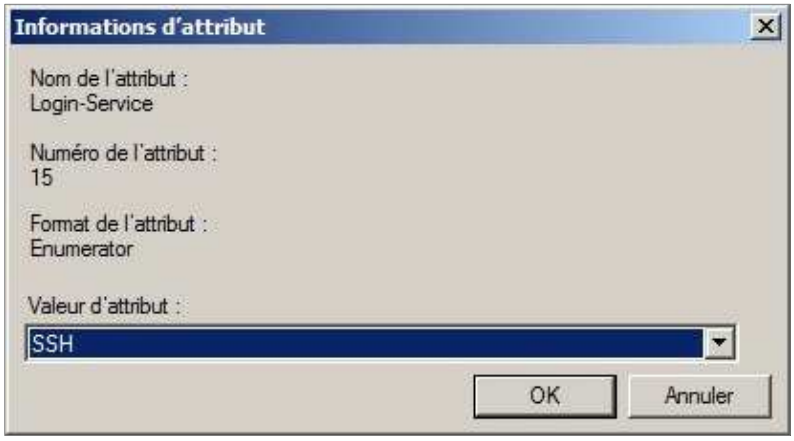
Pour les attributs standards :



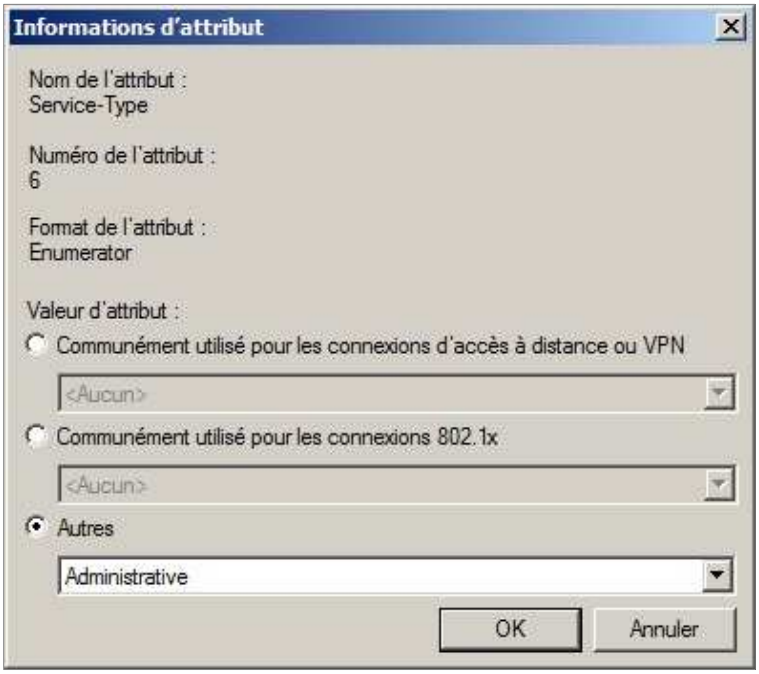
- Ajouter un attribut « Filter-Id » tel que :



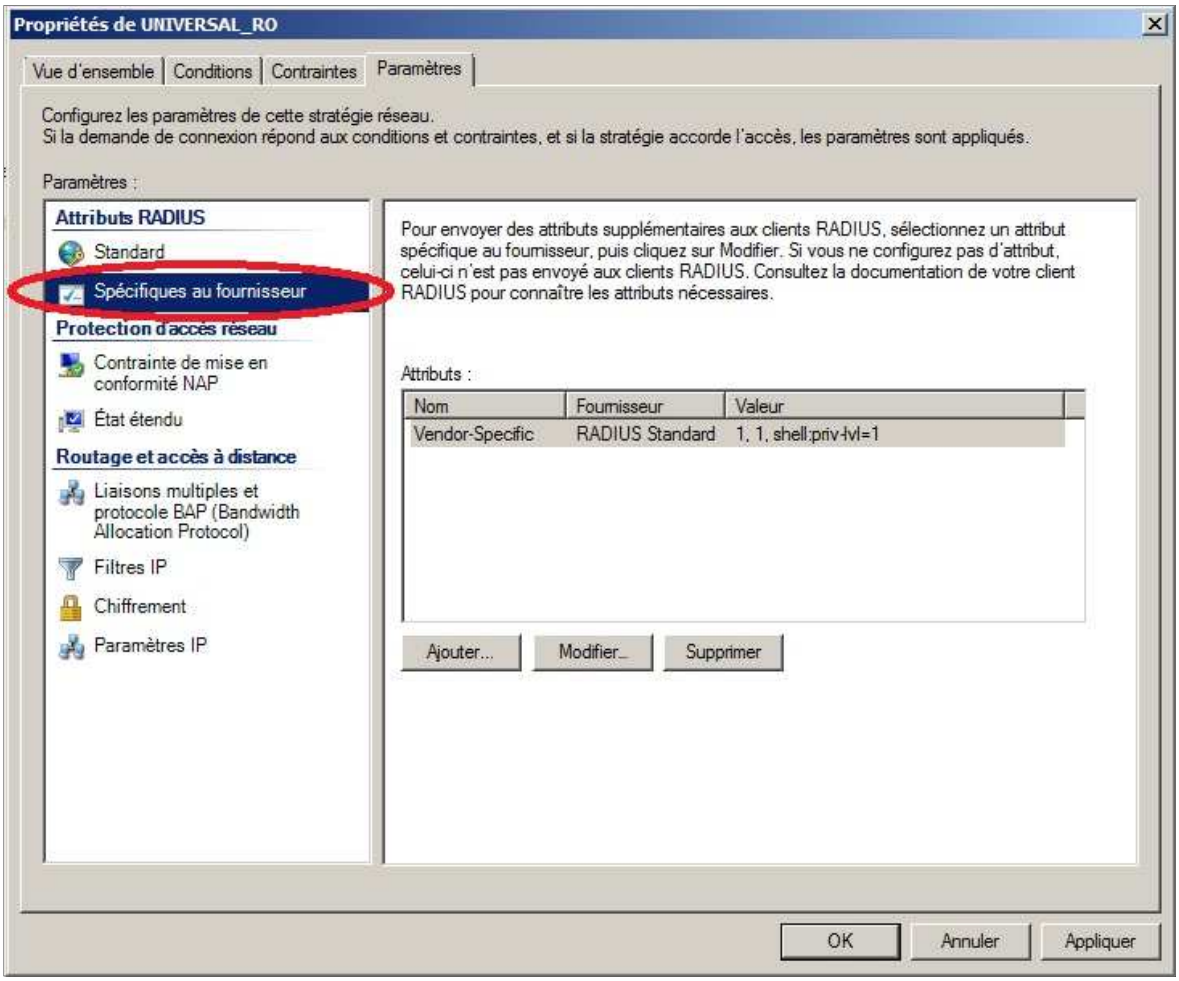
- Ajouter un attribut « Login-Service » tel que :



- Ajouter un attribut « Service-Type » tel que :

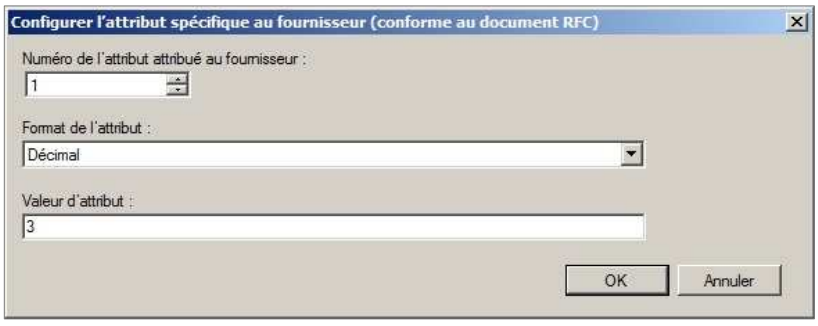


Pour les attributs Spécifiques au fournisseur :



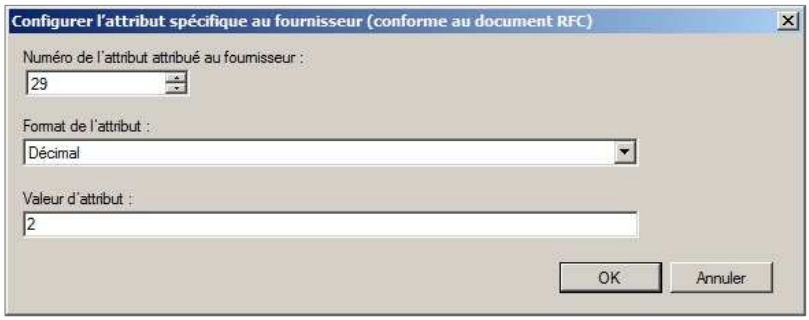
Ajouter trois attributs « Vendor-Specific » tels que :

1)



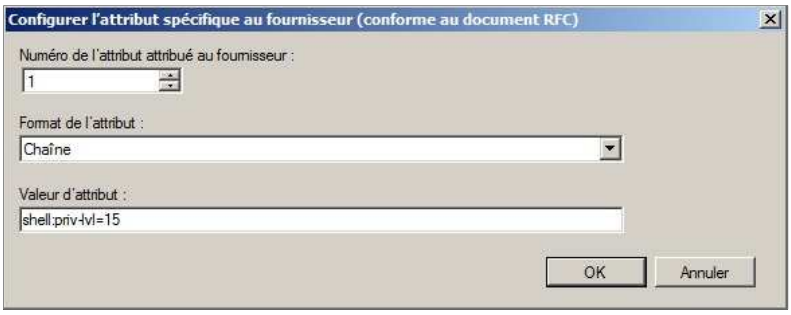
2)


Informations d'attribut spécifiques au fournisseur
Nom de l'attribut :
Spécifique au fournisseur
Spécifiez le fournisseur du serveur d'accès réseau.
Effectuez une sélection dans la liste :
RADIUS Standard
Entrez le code du fournisseur :
2011
Indiquez si l'attribut est conforme au document RFC RADIUS pour les attributs spécifiques au fournisseur.
Oui. Il est conforme.
Non. Il n'est pas conforme.
Configurer l'attribut...
OK
Annuler


Configurer l'attribut spécifique au fournisseur (conforme au document RFC)
Numéro de l'attribut attribué au fournisseur :
29
Format de l'attribut :
Décimal
Valeur d'attribut :
2
OK
Annuler

3)


Informations d'attribut spécifiques au fournisseur
Nom de l'attribut :
Spécifique au fournisseur
Spécifiez le fournisseur du serveur d'accès réseau.
Effectuez une sélection dans la liste :
Cisco
Entrez le code du fournisseur :
0
Indiquez si l'attribut est conforme au document RFC RADIUS pour les attributs spécifiques au fournisseur.
Oui. Il est conforme.
Non. Il n'est pas conforme.
Configurer l'attribut...
OK
Annuler


Configurer l'attribut spécifique au fournisseur (conforme au document RFC)
Numéro de l'attribut attribué au fournisseur :
1
Format de l'attribut :
Chaîne
Valeur d'attribut :
shell:priv-lvl=15
OK
Annuler

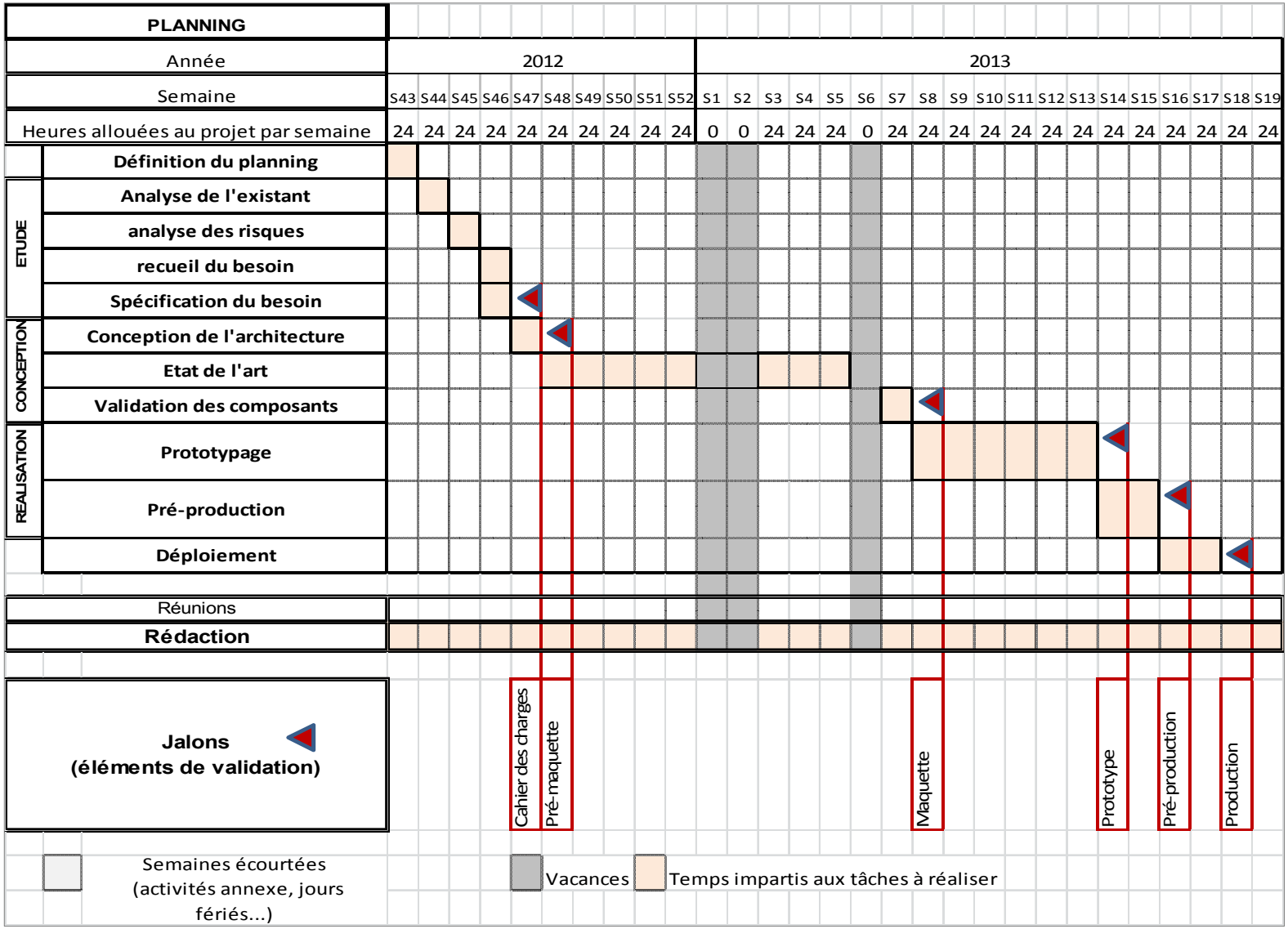
ANNEXE F : SCRIPT DE SYNCHRONISATION DES SERVEURS NPS

```
###Network Policy Server Synchronization Script
#This script copies the configuration from the NPS Master Server and
imports it on this server.
#The Account that this script runs under must have Local Administrator
rights to the NPS Master.
#This was designed to be run as a scheduled task on the NPS Secondary
Servers on an hourly,daily, or as-needed basis.
#Last Modified 01 Dec 2009 by JGrote <jgrote AT enpointe NOSPAM-DOTCOM>
# Traduction SCH GOULAIS 2013

#################################################################################
##################
###Variables
#NPSMaster - Serveur NPS Maitre qui va servir de reference.
$NPSMaster = "DRM-MRNSWA01V"

#NPSConfigTempFile - Repertoire de stockage temporaire du fichier de
configuration XML exportaté. Utiliser un chemin UNC. Vérifier les
permission sur cette ressource, ATTENTION l'export stocke les clefs
prépartagées dans le fichier.
$NPSConfigTempFile = "\\$NPSMaster\e$\export_nps\NPSConfig-$NPSMasterr.xml"
#################################################################################
##################

#Création d'une source d'evenement si elle n'existe pas deja
if (!(get-eventlog -logname "System" -source "NPS-Sync")) {new-eventlog -
logname "System" -source "NPS-Sync"}

#ecrire un message d'erreur et finir le script si un problème apparait
trap {write-eventlog -logname "System" -eventID 1 -source "NPS-Sync" -
EntryType "Error" -Message "An Error occured during NPS Sync: $_. Script
run from $($MyInvocation.MyCommand.Definition)"; exit}

#se connecter au serveur NPS maitre et exporter la configuration
$configExportResult = invoke-command -ComputerName $NPSMaster -scriptBlock
{netsh nps export filename = "e:\export_nps\NPSConfig-$NPSMaster.xml"
exportPSK = yes}

#verification de l'export s'est bien deroule. Si ce n'est aps le cas, creer
un evenement et finir le script.
$NPSConfigTest = Get-Item $NPSConfigTempFile


#supprimer la configuration existante du server NPS secondaire
$configClearResult = netsh nps reset config
$configImportResult = netsh nps import filename = $NPSConfigTempFile

#Effecer le fichier temporaire.
#remove-item -path $NPSConfigTempFile

#journaliser le succes de l'operation
$successText = "Network Policy Server Configuration successfully
synchronized from $NPSMaster.

Export Results: $configExportResult

Import Results: $configImportResult

Script was run from $($MyInvocation.MyCommand.Definition)"
```

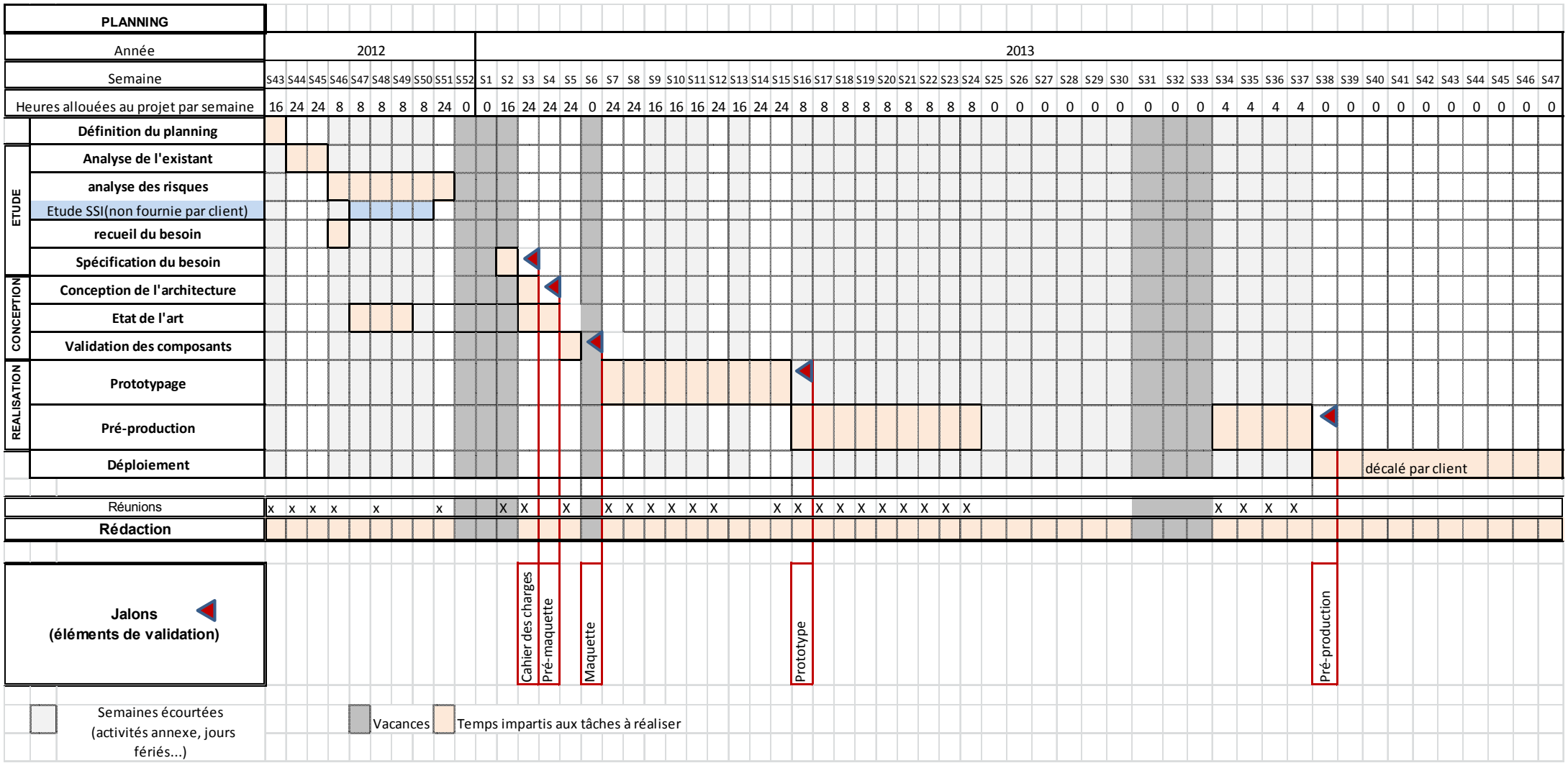
```
write-eventlog -logname "System" -eventID 1 -source "NPS-Sync" -EntryType
"Information" -Message $successText

################################################
#paramètre de la tâche planifiée.
#-noprofile -executionpolicy Unrestricted -file e:\scripts\SyncNPS.ps1
################################################
```

ANNEXE G : PLANNING DU PROJET

Planning initial



Planning réalisé



VII BIBLIOGRAPHIE ET WEBOGRAPHIE

« Réseaux » 4e édition Andrew Tanenbaum

Documentations internes au ministère de la défense (Méthodologie, support de formation, préconisations internes…)

http://www.iana.org/assignments/radius-types/radius-types.xhtml

http://loganalyzer.adiscon.com/

http://www.intersectalliance.com/projects/SnareWindows/

http://www.centos.org/

http://www.rsyslog.com/doc/manual.html

Et bien évidement, suite à mes recherches, de nombreux sites et forums principalement anglo-saxons

VIII LISTE DES FIGURES

IX GLOSSAIRE

AAA : Authentication, Authorization, Accounting = Authentification, Autorisation, Traçabilité (protocoles implémentant ces trois fonctions)

ACSSI *:* Article Contrôlés pour la Sécurité des Systèmes d'Information (éléments concourant à la SSI: Chiffreur, clefs de chiffrement,…)

CNMO : Centre National de Mise en Œuvre (centre de service ayant pour responsabilité le soutien d'une zone géographique étendue : tout ou partie du territoire national.)

DEX *:* division exploitation.

DEX/RZO *:* Cellule réseau de la division exploitation

EAR : Equipement Actif Réseau (éléments actifs en pile)

RH *:* Ressources Humaines

IANA : Internet Assigned Numbers Authority (organisation gérant l'adressage IP d'internet ainsi que les autres ressources partagées de numérotation requises soit par les protocoles de communication sur internet, soit pour l'interconnexion de réseaux à internet).

MOE : Maitrise d'œuvre : partie chargée de la conception et de la conduite opérationnelle d'un projet

OSSI *:* Officier Sécurité des Systèmes d'Information (responsable de la sécurité des systèmes d'information de la formation)

SDK : Service DesK (Centre de Service et d'assistance aux utilisateurs du SI)

SIC : Systèmes d'Information et de Communication

SNMP : Simple Network Management Protocol, protocole permettant la gestion, la supervision et le diagnostic des Equipements Actif Réseau à distance.

SOC : Security Operations Center, centre opérationnel de sécurité. Centre ayant pour fonction principale la supervision de la sécurité.

SSI*:* Sécurité des Systèmes d'Information

TOE : Target Of Evaluation : partie d'un système d'information faisant l'objet d'une analyse de sécurité

WAN : (Wide Area Network, réseaux étendu de transport)

X RESUME ET MOTS CLES EN FRANÇAIS ET EN ANGLAIS

Résumé

Etude et réalisation d'un système d'authentification centralisée et sécurisée visant l'amélioration des contrôles d'accès aux équipements LAN dans le cadre de la télé-administration des matériels

Mémoire d'ingénieur C.N.A.M., Rennes 2014

Mots clefs

AAA / Journalisation / Authentification / Autorisations / Administration Eléments Actifs Réseaux / Eléments Actifs Réseaux / RADIUS / Rsyslog / Loganalyzer

Key words

AAA / Accounting / Authentication / Authorization / Network Equipment Administration / Network Equipment / RADIUS / Rsyslog / Loganalyzer