La supervision active directory

Rodrigue Régis

le cnam

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE REGIONAL ASSOCIE DE VERSAILLES

MEMOIRE

présenté en vue d'obtenir

le DIPLOME D'INGENIEUR CNAM

SPECIALITE : Informatique

OPTION : Réseaux, systèmes et multimédia

par

Rodrigue REGIS

La supervision active directory

Soutenu le 20 mai 2014

JURY

PRESIDENT : M. Kamel BARKAOUI

MEMBRES : M. Georges KERYVEL
M. Emile GEAHCHAN
M. Olivier MANZANO
M. Louis MALLET

Remerciements

Mes remerciements vont dans un premier temps à l'ensemble des collègues d'AXA Technology Services (ATS) avec qui j'ai passé plusieurs années sur la mission. Je n'évoquerai pas des anecdotes ou beaucoup ont voulu imiter mon accent antillais très prononcé, mais n'est pas antillais qui veut. Alors un grand merci à tous.

Je tenais à remercier Vincent JACQUET, salarié d'ATS. Vincent a permis mon intégration au sein de l'équipe IDST[1] Windows. Il m'a formé sur les outils utilisés chez le client ATS. Il a aussi participé au déploiement de la solution de supervision Active directory. Il est un spécialiste comme on aimerait en croiser plus souvent. Un grand merci à Vincent, à ses filles et « Véro », sa compagne.

Je remercie Olivier MANZANO, qui m'a recruté comme prestataire au sein de son équipe. Olivier est un « dénicheur » de talent. Il a su me faire confiance et m'encourager dans mes différents projets, tant personnels que professionnels. Ce projet a été possible grâce a Olivier, à qui je dois beaucoup, car il m'a choisi pour mener à bien cette mission stratégique pour le service. Olivier a été mon tuteur chez ATS, et n'a pas cessé de m'encourager pour que je mène à bien mon projet au CNAM[2].

Un grand merci au CNAM qui m'a permis d'arriver jusqu'ici dans cette aventure. Grâce au CNAM j'ai obtenu le diplôme de licence informatique (Bac+3) et mon diplôme de concepteur architecte informatique (Bac+4). Je remercie tous les enseignants du CNAM qui m'ont offert de leur temps et un enseignement de qualité. Et à tous les centres du CNAM ou j'ai été inscrit tout au long de mon cursus.

Mes remerciements les plus sincères vont à Mr Georges KERYVEL, mon tuteur au CNAM. Il a fait preuve de beaucoup de patience, car souvent j'avais du retard dans mes communications et dans la rédaction de mon mémoire. IL a été de bons conseils dans la rédaction de mon mémoire. Son aide a été très précieuse car j'ai pu profiter de ses conseils avisés en tant qu'enseignant expérimenté au CNAM. Un grand merci à Mr KERYVEL.

Je remercie toute ma famille et surtout ma mère qui n'a pas cessé de me motiver à sa manière. « Tu n'as toujours pas fini ? ». « Non maman, pas encore il manque encore 30 pages». Un grand merci à toute ma famille qui m'a motivé.

Le mot de la fin est pour ma compagne Céline, qui m'a soutenu depuis le début. Elle n'a pas cessé de m'encourager tout au long de ces années. Céline m'a beaucoup motivé pour que j'aille au bout de mon projet au CNAM. Elle a été compréhensive pour me permettre de suivre mes cours, même lorsque je rentrais tard le soir. Merci Céline pour la confiance que tu m'as témoignée. Je remercie aussi ses parents et ses sœurs pour leur soutien.

[1] IDST : Infrastructure, Déploiement, Support et Télédistribution
[2] CNAM : Conservatoire National des Arts et Métiers

Sommaire

Liste des figures

Liste des tableaux

I Présentation générale

AXA Technology Services ou ATS est une société filiale du groupe AXA. Elle est chargée de gérer l'infrastructure informatique d'AXA dans le monde. Le groupe AXA utilise des processus de gestion de la qualité et de traçabilité pour une meilleure communication avec ses clients.
Au sein du groupe AXA, le service d'annuaire pour les serveurs ou stations de travail fonctionnant sous Microsoft Windows est Active Directory (AD). L'Active Directory est un rôle (ou fonction) spécifique installé(e) sur un ou plusieurs serveurs. Ce serveur porte le nom de « contrôleur de domaine ».
ATS est garant du bon fonctionnement de l'Active Directory et doit tenir compte de l'impact des incidents en fonction des différents fuseaux horaires. La surveillance ou la supervision de ce service d'annuaire permet d'identifier tous les éventuels disfonctionnements et d'alerter les équipes d'exploitation.

Des outils de supervisions existent sur le marché et sont utilisés par de grandes entreprises. Ils permettent d'avoir un état complet de l'architecture informatique. La gestion et la mise en place de ces outils nécessitent toutefois des compétences bien spécifiques pour une supervision efficace. Ces outils de supervision ont un coût non négligeable sur le budget du système d'information. Bien que ces outils soient installés chez ATS, les équipes techniques en charge de l'Active Directory ont rencontré de nombreux incidents suite à des défaillances non détectées. De nombreux incidents ont été constatés entre 2011 et 2012 le plus souvent par les utilisateurs. Le responsable de l'équipe, Olivier Manzano a souhaité une supervision plus efficace et être alerté directement en cas de défaillance de l'AD[3]. Pour chaque incident détecté un ticket de suivi sera créé dans l'outil outil de gestion des incidents d'ATS.
J'ai été chargé par Olivier Manzano de mettre en place un système de supervision fait sur mesure. J'interviens donc comme maîtrise d'œuvre (MOE) sur le projet. Le budget de réalisation du projet est celui de fonctionnement du service. Le projet doit prendre en compte toutes les versions serveurs de Microsoft Windows composant l'infrastructure technique chez ATS.
Les outils utilisés devront être natifs à Windows et ne nécessiteront pas de nouvelles installations : pas de logiciels récupérés sur Internet qui pourraient présenter des failles de sécurités. Les activités des clients d'ATS sont très sensibles et génèrent des chiffres d'affaires très importants.

Afin de respecter les exigences en matière de sécurité, les programmes ont été développés en langage Visual Basic Script (VBS). Les codes sources sont exploitables par tous les programmeurs et pourront être audités par les services de la sécurité interne d'AXA. Certains outils sont disponibles nativement sous Windows, récupérables gratuitement sur le site de Microsoft et dans les outils d'administration de Windows. Le code source pourra être modifié afin d'évoluer en fonction des nouveaux besoins de l'entreprise.
Une analyse des différents incidents rencontrés durant plusieurs mois, a permis d'établir les points essentiels à superviser pour le bon fonctionnement du service d'annuaire. Bien que certaines causes soient de nature différentes, les conséquences sur la supervision seront les mêmes. Nous ne chercherons donc pas forcément la cause exacte de l'anomalie, mais uniquement à alerter lors de l'apparition de cette anomalie. Ainsi, une panne d'un équipement réseau ou une coupure électrique sera traitée de la même manière. Certaines ressources

[3] AD : Active Directory

internes ou externes à l'entreprise ne seront pas accessibles par les utilisateurs. Ces ressources peuvent être de nature diverses : site intranet ou Internet, serveurs de fichiers, applications, réseaux…
Les points les plus bloquants ont été retenus pour la supervision de l'infrastructure active directory.

- Les services Windows
- L'authentification des comptes
- La résolution des noms DNS[4]
- Compte d'installation des serveurs

Tous les points ci-dessus seront testés sur l'ensemble des contrôleurs de domaine gérés par ATS. Avec plus de 50 domaines et 200 contrôleurs de domaines, j'utiliserai l'ordonnanceur TWS[5] d'IBM[6] pour gérer la supervision des serveurs. Un ordonnanceur est un outil qui fonctionne comme le planificateur de taches sous Windows. Son rôle sera d'exécuter les différents programmes de la supervision à intervalle régulière. La supervision sera centralisée sur un seul contrôleur de domaine de chaque domaine. Ce contrôleur de domaine sera le point faible de la supervision. Mais l'ordonnanceur utilisé est capable de générer lui aussi un ticket d'incident si une erreur d'exécution de la tache a été détectée. Ce qui permet de compenser cette faiblesse. L'ordonnanceur sera l'élément incontournable du projet.
Les résultats de tous les tests seront comparés à un résultat attendu. Lorsque les résultats ne seront pas conformes, un ticket d'incident sera généré dans la base de suivi des incidents du groupe AXA. Le ticket de suivi de l'incident aura un numéro interne pour son suivi et sa résolution. Ce ticket comportera les éléments essentiels pour son traitement par les équipes d'exploitation. Les équipes recevront en parallèle un courriel les informant de l'incident sur l'infrastructure AD. Tous les moyens seront utilisés pour être le plus réactif possible à l'apparition d'une anomalie.
La solution que je propose à ATS est générique, c'est-à-dire utilisable sans modifier les codes sources. Tous les éléments de personnalisation ont été positionnés dans les fichiers de configurations. Les informations relatives aux serveurs à superviser seront renseignées dans ces fichiers. Des plages de maintenances ont été prévues dans la supervision afin de permettre de réaliser les opérations périodiques de nuit. Il n'est donc pas nécessaire d'intervenir sur la supervision lors de ces opérations. Il est aussi possible de désactiver temporairement la supervision de certains serveurs de l'infrastructure en agissant directement dans ce même fichier de configuration.
Lors de chaque cycle de supervision, c'est-à-dire un test complet de tous les serveurs à superviser, des fichiers d'exploitation seront consolidés. Il existe deux types de fichiers. Un fichier historique qui garde tous les traitements, et pourra servir à des fins de statistiques si besoin. Il sert aussi à contrôler les incidents durant la plage de maintenance, hors plage horaire de production. Un fichier journal, qui donnera l'état à l'instant « t » de l'infrastructure. Ce fichier journal, servira à la cartographie de l'infrastructure qui ne fait pas partie de ce projet.

Le projet a permis de détecter à ce jour plus d'une centaine de disfonctionnements majeurs sur l'infrastructure du groupe AXA. Les conséquences pour les utilisateurs ont été limitées, voire complètement transparentes, grâce à la réactivité des équipes d'exploitation.

[4] DNS : Domain Name Server
[5] TWS : Tivoli Workload Scheduler
[6] IBM : International Business Machines, société internationale

Le coût de ce projet a été limité au budget de fonctionnement du service. Les programmes de la supervision ne sont pas soumis à des licences d'exploitation. Ainsi, des économies importantes ont été réalisées.
Ce projet a permis de gagner la confiance des utilisateurs en leur proposant une infrastructure maîtrisée et sous contrôle. Les remontées d'incidents majeurs sur l'infrastructure active directory par les utilisateurs sont devenues quasi-inexistantes.
Le projet a été couronné d'un grand succès. Des axes d'améliorations ont été recensés, mais restent à ce jour non implémentés.

Le document est architecturé en quatre parties. Dans la première partie, nous aborderons la surveillance des systèmes informatiques. Cette partie traitera de la place de l'informatique dans l'entreprise. La seconde partie, traitera de la mise en place de la supervision d'active directory. Les différents aspects de la supervision informatique seront abordés. La troisième partie traitera de la réalisation de l'outil de supervision. L'architecture logicielle sera décortiquée. La quatrième partie, la conclusion, qui fera le bilan global du projet.

II La surveillance des systèmes informatiques

Les technologies ont beaucoup évolués durant ces dernières années. Les infrastructures d'entreprise sont de plus en plus complexes. La tendance actuelle est la réduction des coûts d'exploitation tout en délivrant des services de qualité. La standardisation des processus d'industrialisation permet d'optimiser les offres de services et d'être compétitif.
La multiplication des offres de services nécessite des infrastructures performantes et disponibles en permanence. L'Active directory est le service d'annuaire qui permet d'accéder aux différentes ressources de la société. Les incidents sur l'architecture Active Directory peuvent avoir des conséquences importantes sur le fonctionnement de l'entreprise. Ils ont considérablement affectés la confiance des utilisateurs et de la direction du groupe AXA. Les outils de supervision utilisés jusque là, n'avaient pas permis de détecter certains incidents.
L'Active Directory est un composant important de l'architecture du système d'information de l'entreprise. La surveillance de ce service d'annuaire et de ses composants permet d'être réactif et de limiter les conséquences. Lors l'apparition d'une anomalie ou d'un incident, les équipes d'exploitation seront alertées : par courriel, via un outil de gestion d'incidents, etc.
Un outil de supervision, contrôle l'état des composants sur un serveur, si le résultat de ce contrôle n'est pas conforme à celui attendu, une alerte sera déclenchée.
Le responsable du service IDST Windows a souhaité mettre en place une supervision faite sur mesure, qui réponde au besoin de l'entreprise.
En tant que membre de l'équipe IDST Windows, j'ai été désigné comme MOE pour le projet.

II.1 Présentation de la société

AXA Technology Services ou ATS est une société filiale 100% du groupe AXA. Elle est le fruit de la consolidation des équipes en charge de l'infrastructure informatique dans les différentes sociétés du Groupe AXA. La société ATS est spécialisée dans la gouvernance informatique. Sa mission est d'offrir des services de système d'exploitation. Elle utilise des méthodes de gestion de qualité et des indicateurs de performances qu'elle communique à ses différents clients. Elle se base sur norme ISO 9001 qui donne les exigences relatives au système de management de la qualité.
ATS compte plus de 800 collaborateurs répartis dans différents pays. Le groupe AXA compte 120 000 salariés dans le monde.
ATS utilise des technologies de pointe afin d'offrir des services de qualités à l'ensemble de ses clients. Ces technologies nécessitent des compétences spécifiques et des partenariats avec les plus grands éditeurs :

- Microsoft : éditeur de systèmes d'exploitation et de solutions applicatives
- Computer Associates : éditeur de logiciels, solution de sécurités, etc.
- IBM : fournisseur de matériels informatiques et éditeur de logiciels
- etc.

La priorité d'ATS est de rendre un service de qualité à ses clients tout en réduisant les coûts auprès des différents partenaires et fournisseurs. Elle profite de la puissance de recherche et développement de ses partenaires pour fournir des services innovants ses clients.

II.1.1 Les clients et leurs exigences

Les clients d'ATS sont des filiales du groupe AXA. Certains clients ont des spécificités juridiques particulières qui nécessitent des infrastructures informatiques séparées du reste du groupe. Ces contraintes juridiques obligent à multiplier les infrastructures tout en garantissant un niveau de service très élevé. Les activités des clients d'ATS sont nombreuses : assurance, mutuelle, conseil, banque, etc. Il convient donc de respecter les exigences liées à ces différents métiers. La réactivité des équipes techniques permet de gagner la confiance des clients.
ATS propose à ses clients un accompagnement personnalisé pour leur permettre d'utiliser plus efficacement les technologies mises à leur disposition.
Elle utilise des processus métiers visant à accroître sa qualité de service. Au travers la gestion du changement, elle garantit à ses clients l'utilisation de bonnes pratiques dans le respect des normes et des standards. La norme ISO 9004 fourni les lignes directrices pour l'amélioration continue.

II.1.2 Une couverture internationale

ATS a une couverture internationale du fait des activités de ses clients et ses collaborateurs basés dans différents pays. Afin d'être plus performante, elle a regroupé ses activités autour de 5 régions :

- Amérique du Nord (Etats-Unis, Mexique)
- Europe du Nord (Allemagne, Belgique)
- Europe Centrale et Japon (Royaume Uni, Suisse, pays de l'Est et Japon)
- Europe du Sud (France, Italie, Espagne, Portugal, Maroc)
- Asie (Hong-Kong, Singapour, Indonésie)

La législation dans les différents pays n'étant pas la même, elle est soumise à des obligations de transparence en matière de gestion de l'information. Des audits chez ses clients peuvent avoir des répercutions sur son activité : archivages des données, audit des accès, etc.
Le savoir faire et la taille de son infrastructure informatique font d'ATS un des acteurs importants sur la scène internationale.

II.1.3 ATS, fournisseur de services

ATS est un fournisseur de services aux activités variées. Elle propose :

- Des solutions de stockage, disque réseaux, serveurs de fichiers
- L'hébergement de site web, l'hébergement applicatif, etc.
- L'accès à Internet et l'accès à l'environnement de travail depuis internet.
- Du conseil : accompagnement des clients
- Des audits techniques : supports niveau 1, 2 et 3
- etc.

Les clients les plus exigeants ont des infrastructures qui leur sont dédiées. Les autres clients partagent des infrastructures dites « infrastructures mutualisées ».
Les technologies ont beaucoup évolué durant ces dernières années. ATS s'engage à fournir à ses clients des technologies de pointes, tout en garantissant un très bon niveau de service. Le niveau de service est défini par contrat de service avec des indicateurs de suivi :

- Disponibilité
- Performance
- Accessibilité
- Etc.

Les infrastructures doivent être supervisées afin d'être réactif si un ou plusieurs de ces indicateurs de suivi étaient impactés. La supervision permet de détecter les anomalies et de réduire les conséquences sur la production.

II.1.4 Le contexte

Le projet s'inscrit dans un projet de qualité de service autour de l'infrastructure Active Directory. L'infrastructure est composée exclusivement de systèmes d'exploitation Microsoft Windows. Le service **IDST**[7] **Windows**, l'équipe technique en charge de l'infrastructure technique, gère plus de 200 contrôleurs de domaines.
L'infrastructure est répartie de la manière suivante :

- 30 domaines de production
- 20 domaines de pré-production (hors production)

Les versions Windows 2000, 2003 et 2008 serveurs cohabitent dans l'infrastructure.
Le service **IDST Windows** en charge de l'infrastructure active directory est le point stratégique chez AXA.

II.1.4.1 Le service IDST Windows un maillon centrale

Le service IDST Windows est positionné au cœur de l'activité informatique du groupe AXA. Il est le point d'entrée vers les différents fournisseurs et les supports de niveau 3. Le savoir faire et les compétences des collaborateurs du service sont reconnus par tous ses clients.

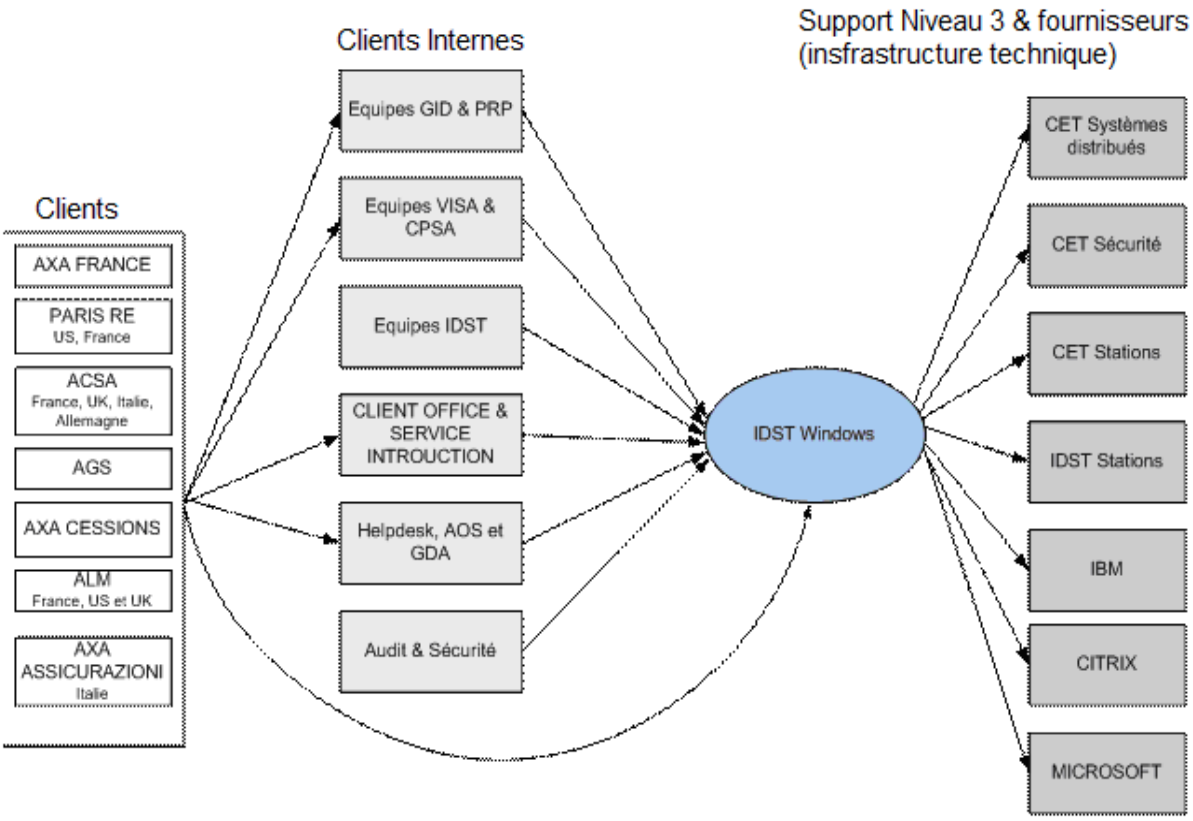


Figure 1 : Positionnement du service IDST Windows chez AXA

[7] IDST : Infrastructure, Déploiement, Support et Télédistribution

II.1.4.2 Positionnement dans le service IDST Windows

Le service IDST Windows est composé de trois pôles de compétences. Le service est dirigé par Olivier Manzano, ingénieur CNAM.
Les trois pôles de compétences sont répartis de la manière suivante

- Pôle Citrix
- Pôle Infrastructure Système
- Pôle outils collaboratifs

Chaque pôle placé sous la responsabilité d'un coordinateur de pôle qui rapporte directement à Olivier Manzano.

Je fais parti du pôle Infrastructure système. Mes compétences variées m'ont permis de participer à des projets gérés par le pôle Outils collaboratifs. Le Service Outils collaboratifs est en charge de la gestion de l'active directory. C'est dans ce contexte que le responsable du service m'a confié le projet de renforcement de la surveillance de l'active directory.

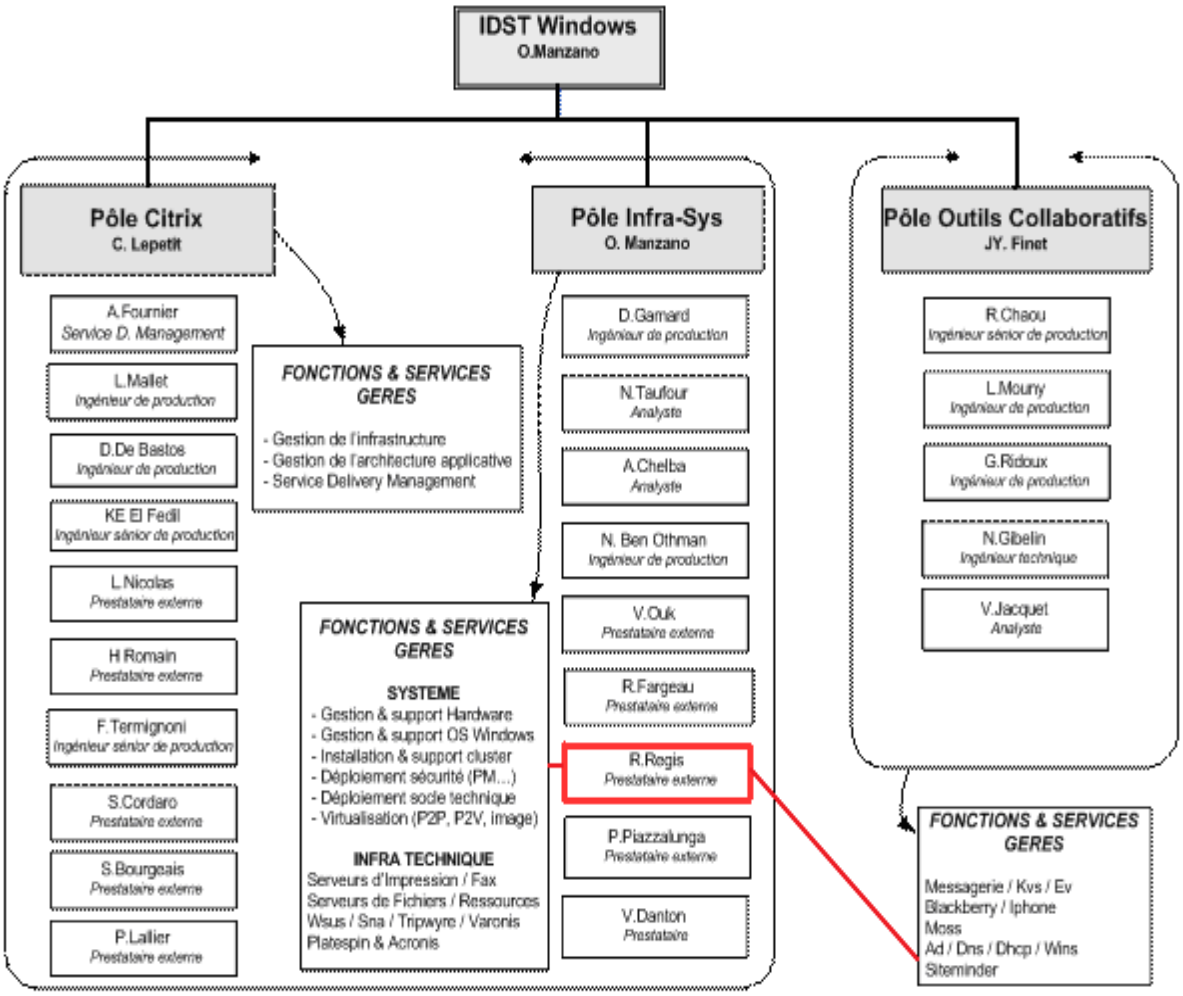


Figure 2 : Organigramme du service

II.2 La stratégie de l'entreprise

ATS a misé sur la relation clients et la transparence, en plaçant ses clients et ses actionnaires au centre de ses préoccupations.

II.2.1 La politique de transparence

ATS met tout en œuvre afin de fournir un système d'information qui réponde aux exigences de ses clients. La traçabilité des opérations sur l'infrastructure a atteint un niveau de maturité.
Les clients d'ATS participent aux comités de validation des changements. Elle propose un accompagnement personnalisé à ses clients.
Les clients ont une visibilité sur les différentes opérations terminées, en cours ou programmées. ATS communique quotidiennement à ses clients la liste des incidents majeurs pouvant influencer leurs activités. Des statistiques sont aussi communiquées aux différents interlocuteurs des domaines métiers.
La recherche des causes ne s'arrête pas à la seule résolution de l'incident. Le comité de **comptes rendu des incidents majeurs** (**CRIM**), suit l'ensemble des incidents majeurs et tente de déterminer les responsabilités : erreur humaine, matériel, fournisseurs… Les incidents majeurs, sont des incidents ayant un impact important sur le business ou les activités des clients. Les incidents majeurs sont classés selon deux niveaux : P1 ou P2, décrit dans le paragraphe II.2.2.
Les incidents du type P1 font systématiquement l'objet d'une communication et d'un compte rendu détaillé aux clients.
La gestion des incidents et des changements dans une base commune permet d'établir des liens entre chaque opération planifiée sur l'infrastructure et les incidents déclarés. Toutes les informations sont regroupées dans une seule et même base.

II.2.2 La gestion des incidents et la traçabilité

Tous les incidents doivent être obligatoirement saisis dans la base de suivi des incidents. Ils peuvent être initiés à la demande des utilisateurs selon les différents moyens mis à leur disposition :

- Téléphone : appel vers un numéro unique, un opérateur prend en compte l'appel et ouvre un ticket pour l'incident.
- Par courriel : des opérateurs saisissent l'incident dans le logiciel de gestion d'incidents à partir des informations reçues dans le courriel.
- Logiciel : directement dans l'outil de gestion des incidents
  - Saisie utilisateurs
  - Automatise d'ouverture d'incidents

Chaque incident possède un numéro unique avec les informations permettant la qualification de l'incident et d'identification de l'utilisateur concerné.
Les incidents sont classés en plusieurs niveaux de priorité :

- P1 : incident majeur bloquant, impactant le fonctionnement de l'entreprise.
- P2 : incident majeur impact de nombreux utilisateurs
- P3 : incident affectant au moins un utilisateur
- P4 : incident affectant ou pouvant affecter un seul utilisateur

ATS a souhaité la création automatiquement des tickets de suivi des incidents dans son outil de gestion des tickets par tous les outils de supervisions. Chaque incident détecté sera

référencé par un ticket en priorité P3 (voir ci-dessus). C'est à la charge de l'équipe exploitante de changer le niveau de priorité en accord avec les gestionnaires des incidents majeurs.

La figure 3, montre différents cas de figure auxquels les utilisateurs sont le plus souvent confrontés lors de l'apparition d'un incident.

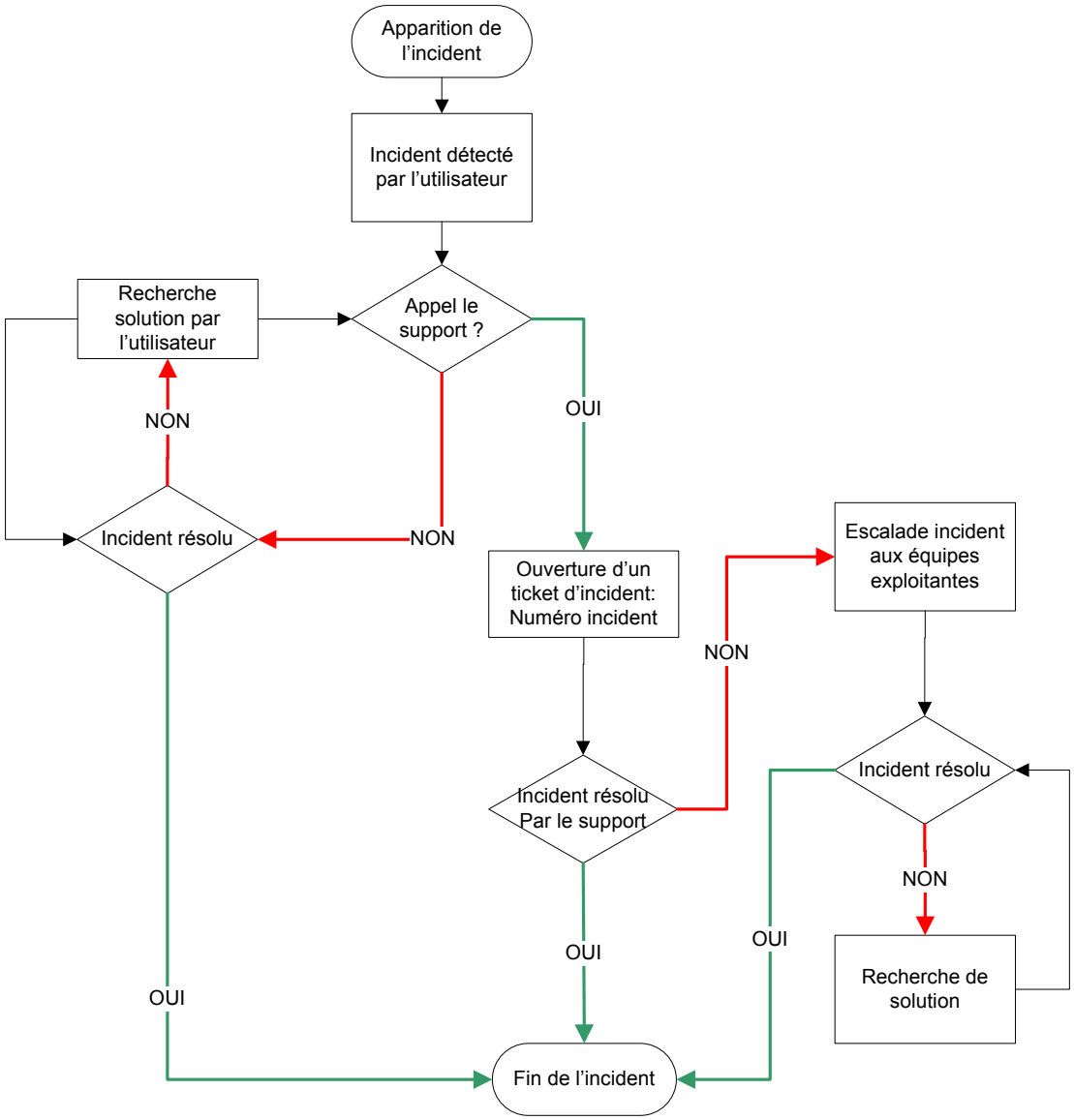


Figure 3 : La détection d'un incident par un utilisateur.

Le processus de gestion d'un incident, n'affectant qu'un seul utilisateur, peut différer selon la politique interne de la société.
Les incidents majeurs du type P1, font l'objet d'une attention toute particulière. Elles sont souvent à l'origine de remontée de nombreux utilisateurs pour des incidents ayant des causes communes.
La durée de traitement maximale des différents niveaux d'incidents est fixée par des contrats de service. Le décompte débute généralement lors de la création du ticket d'incident par le support.

II.2.3 Contrat de services

Axa Technology Services, en relation avec ses clients et partenaires, a mis en place un contrat de niveau de service appelé SLA[8] en anglais. Les applications sont référencées et des plages disponibilités d'utilisation sont communiquées à l'ensemble des équipes techniques.
ATS a établi des SLA avec 13 partenaires couvrant 166 applications majeures, voir le tableau 1. ATS gère un total de 18 applications majeures qui fonctionnent en 24h/24h et 7j/7j. Ce contrat de niveau de qualité de service a un intérêt stratégique dans l'engagement de la qualité de service d'ATS. Il permet de maintenir la confiance de ses clients et de pérenniser les avoirs des actionnaires.
La liste des applications majeures est réalisée en fonction de critères définis avec les clients et les risques sur le business. Elle sert à établir le niveau de criticité des incidents et d'évaluer les risques opérationnels. Ainsi lorsqu'une application est indisponible, il est possible d'évaluer les pertes engendrées et d'être plus réactifs dans le traitement des incidents.
Le contrat de service engage la responsabilité de la DSI. Le non respect des engagements du contrat de services peut avoir des influences importantes sur l'activité des clients. Des statistiques sont fournies aux clients sur la disponibilité des applications, de manière :

- Hebdomadaire
- Mensuelle
- Annuelle

La liste complète des applications majeures est fournie en annexe 6.

Clients / Partenaires	Applications majeures	Horaires : 7j/7 24/24
AXA Assistance	7	7
AXA Banque	10	2
AXA Corporate Solutions	15	0
AXA Protection Juridique - Juridica	1	0
GIE AXA	11	0
AXA Direct Protection	6	1
AXA LM	9	0
AXA Tech Corp	6	0
AXA Group Solution (AGS)	22	2
AXA Life Invest	5	0
AXA Global Life & AXA Global P&C	7	0
AXA Global Direct France	5	0
AXA France	62	6
Total:	166	18

Tableau 1 : Partenaires et applications majeures

[8] SLA : Service Level Agreement ou contrat de niveau de service en français

II.2.4 Les impacts métiers et la gestion du risque opérationnel

Les impacts métiers sont souvent difficiles à évaluer dans l'entreprise. La connaissance des métiers de chaque client permet d'identifier les activités critiques. Une liste des applications majeures a été créée et publiée par ATS. Elle permet de afin de quantifier les pertes financières en cas d'indisponibilité du système d'information.
Les impacts liés à l'indisponibilité du système d'information doivent être mesurés. Le risque opérationnel zéro n'existe pas dans la gestion de l'infrastructure informatique. Les interventions sur l'infrastructure de production, serveurs, équipements réseaux, téléphonie et applications, sont formalisées par une demande de changement. Elles sont soumises à l'accord des clients. Les risques sont exposés aux clients concernés lors du Comité d'Approbation des Changements appelé CAB.
Il existe deux types de changement chez ATS :

- changement standard
  - pour les opérations courantes sans risque majeur qui ne nécessitent pas de validation
- changement normal
  - pour les opérations à risque avéré, risque potentiel ou le risque opérationnel n'est pas connu. La validation du responsable client et de la DSI sont obligatoires.

Le processus de gestion du changement ne permet pas d'éliminer les risques, mais de s'assurer que le changement sera réalisé dans le respect des méthodes, procédures et processus standardisés. La gestion des changements est abordée dans la norme ISO 20000. La norme ISO 20000 spécifie les exigences destinées aux fournisseurs de services en matière de gestion des services.

ATS s'engage, auprès de ses clients partenaires, à utiliser de bonnes pratiques dans la gestion de son système d'information. Les moyens mis en œuvre permettent de délivrer des services de qualités.
Ainsi on peu lire sur de nombreux documents et site web du groupe AXA la devise suivante :
«. *Il est de notre responsabilité d'utiliser nos compétences, nos moyens et notre expertise en matière de gestion des risques pour œuvrer à une société solide et sûre*.
Être une entreprise responsable, c'est avant tout écouter les attentes de nos clients, gérer nos risques avec professionnalisme, traiter nos partenaires équitablement et créer un cadre de travail fondé sur la confiance, la diversité et des valeurs fortes. Nos engagements portent en outre sur la protection de l'environnement et le soutien des communautés au travers de la recherche et de l'éducation pour la réduction des risques ». Source, Axa

ATS est garant de la continuité de service en proposant un système d'information qui doit répondre aux exigences définies dans son SLA. L'active directory est le service d'annuaire de l'entreprise, le cœur de l'infrastructure pour les systèmes Microsoft Windows. La supervision de l'architecture active directory doit être mise en œuvre afin de réduire les risques sur le fonctionnement de l'entreprise.

II.3 Le besoin de supervision

Les systèmes informatiques occupent une place de plus en plus importante dans les entreprises. Les outils informatiques sont des moyens d'échange d'informations qui permettent de gagner en réactivité.
Les entreprises ont besoin de connaître l'état de fonctionnement de leurs infrastructures informatiques. Les équipements et les composants sensibles de l'infrastructure ne doivent pas subir d'avaries pouvant perturber le business de l'entreprise. Le service d'annuaire de l'entreprise, l'Active Directory, est un des composants sensible à surveiller.
La supervision informatique permet de s'assurer du bon fonctionnement des systèmes. Elle donne une vision globale de l'état des systèmes. La supervision automatise les tests répétitifs et elle alerte en cas de disfonctionnement.
Il existe de nombreux outils de supervision sur le marché, fonctionnant tous sur les principes avec ou sans agents, décrits au paragraphe II.3.3.

II.3.1 L'active Directory dans l'entreprise

L'active directory est le service d'annuaire qui centralise les ressources de l'entreprise. Il est un des points critiques de l'architecture informatique de l'entreprise. L'active directory est apparu avec Windows 2000 serveur en février 2000. Il a évolué avec les différentes versions de Windows serveur, mais le principe de base n'a pas changé.
L'active directory est un rôle spécifique installé sur un serveur Microsoft Windows. Ce serveur est appelé contrôleur de domaine.

II.3.1.1 Les indispensables dans l'active directory

Un domaine au sens active directory est un annuaire distribué. Il est répliqué ou distribué entre plusieurs serveurs, appelé contrôleurs de domaine.
La gestion des objets dans l'active directory nécessite l'utilisation du protocole LDAP[9]. LDAP est un protocole de communication basé sur la norme X500. La norme X500 vit le jour fin des années 1980. Elle est décrite dans la norme ISO 9594. LDAP est une version allégée et revue du protocole DAP[10], issue de la norme X500. Le tableau ci-dessous est un extrait de la correspondance de la norme X500 et ISO[11] 9594.

Numéro UIT[12]	Numéro ISO/CEI	Titre du Standard
X.500	ISO/CEI 9594-1	Vue d'ensemble des concepts, modèles et services
X.501	ISO/CEI 9594-2	Modèles
X.509	ISO/CEI 9594-8	framework d'Authentification

Tableau 2 : Correspondance de la norme X500 et ISO9594

Dans l'active directory, les objets sont classés et hiérarchisés. Les principaux objets sont repris dans le tableau 3. Lorsque des applications s'intégreront dans l'infrastructure active

[9] LDAP : Lightweight Directory Access Protocol = Protocole d'accès d'annuaire léger
[10] DAP : Directory Acces Protocole
[11] ISO : International Organization for Standardization
[12] UIT : Union internationale des télécommunications

directory, ils peuvent créer de nouveaux objets. Ces objets ne seront pas présentés dans le cadre de ce mémoire.

Icône	Objet	Description
	Utilisateur	Un objet utilisateur est un objet principal de sécurité de l'annuaire. Un utilisateur peut se connecter au réseau avec ces informations d'identification et disposer d'autorisations d'accès.
	Contact	Un objet contact est un compte qui ne dispose d'aucune autorisation de sécurité.
	Ordinateur	Un objet qui représente un ordinateur sur le réseau. Pour les stations de travail et serveurs Windows NT, il s'agit du compte d'ordinateur.
	Unité d'organisation	Les unités d'organisation (UO) sont utilisées comme conteneurs pour organiser de façon logique des objets d'annuaire tels que les utilisateurs, les groupes et les ordinateurs. Elles sont comparables aux dossiers que vous utilisez pour organiser les fichiers sur votre disque dur.
	Groupe	Les groupes peuvent contenir des utilisateurs, des ordinateurs et d'autres groupes. Ils simplifient la gestion d'un grand nombre d'objets.
	Dossier partagé	Un dossier partagé est un objet réseau qui a été publié dans l'annuaire.
	Imprimante partagée	Une imprimante partagée est une imprimante réseau qui a été publiée dans l'annuaire.

Tableau 3 : Les objets de l'active directory, source Microsoft

L'identification des objets dans l'active directory se fait par différents moyens :

- Par le SID[13] (décrit ci-dessous)
- Par le GUID[14] (décrit ci-dessous)

- **Le SID ou identificateur de sécurité**
  Un identificateur de sécurité ou SID est une valeur unique qui permet d'identifier une entité de sécurité ou un groupe de sécurité. La composition du SID est la combinaison de :
  - Du SID du Domaine, identique pour un même domaine
  - D'une partie variable et unique pour chaque domaine, appelé RID[15], pour Identifiant Relatif. Le RID est fourni par le Maître RID, voir tableau 6.

  ⇒ exemple de SID utilisateur : S-1-5-21-720046166-932014646-600732497-XXXX
  SID domaine RID

[13] SID : Secure IDendifier (identificateur de sécurité en français)
[14] GUID : Globally Unique Identifier (Identificateur Globalement Unique en français)
[15] RID : Relative Identifier (Identifiant Relatif en français)

Le SID peut changer quand l'objet est déplacé dans un autre domaine. Mais l'ancien SID est copié dans les propriétés de l'objet dans le champ SID-History (Historique du SID).

Microsoft, sans doute dans un souci de gestion de ses systèmes d'exploitation, a créé des objets avec des SID figés. Le développement de certaines applications peut être simplifié.
Le tableau 4 fournit quelques SID connus.

Valeur SID	Nom	Type	Description
S-1-1-0	Tout le monde	Groupe	Un groupe qui inclut tous les utilisateurs, même les utilisateurs anonymes et les invités
S-1-5-21-domaine-500	Administrateur	Utilisateur	Un compte d'utilisateur de l'administrateur système
S-1-5-21-domaine-513	Utilisateurs du domaine	Groupe	Un groupe global qui, par défaut, inclut tous les comptes d'utilisateur dans un domaine
SID: S-1-5-21-domaine racine-518	Administrateurs du schéma	Groupe	Le groupe est autorisé à apporter des modifications de schéma dans Active Directory

Tableau 4 : Exemple de SID connus, source Microsoft[16]

- **Le GUID**
  Chaque objet est identifié par son Identificateur Globalement Unique (GUID). Cet Identificateur est généré lors de la création de l'objet. Il est unique, non seulement dans la société, mais aussi dans le monde, d'après les sources Microsoft[17]. La valeur du GUID est de 128 bits, soit 2^{128} combinaisons possibles.
  Le GUID d'un objet, contrairement au SID, ne change jamais, même en cas de migration vers un autre domaine.
  Un exemple de GUID : **e35e82a15-dccb-22c3-e19f-00a52e7de503**

Dans la gestion des listes de contrôles d'accès, appelé ACL (Access Control List en anglais), le SID est utilisé pour l'autorisation ou le refus d'accès à une ressource. Dans le cas d'un objet ayant un SID-History renseigné, il sera aussi vérifié pour le contrôle d'accès.

- **Authentification NTLM et Kerberos**
  - **NTLM:** New Technology Lan Manager est un protocole d'authentification utilisé par défaut par Microsoft Windows. Sa version initiale LM (LanManager) a été développée par IBM. NTLM est toujours utilisé pour des raisons de compatibilité avec les anciens systèmes. Il faut noter que ce protocole ne traverse pas les pare-feux et proxy. L'architecture réseau déterminera les ou les cas d'utilisation de ce protocole.

  - **Kerberos:** Est un protocole authentification fort basé sur des clés symétriques. Ce qui implique l'installation de certificats de cryptage pour les échanges. Son avantage est

[16] Consultable sur le site de microsoft: http://support.microsoft.com/kb/243330/fr
[17] Consultable sur le site de microsoft: http://technet.microsoft.com/en-us/library/cc961625.aspx

de ne transmettre aucun mot de passe en clair sur le réseau. Kerberos utilises le type de cryptage DES (Data Encryption Standard).

Des informations complémentaires sur l'authentification NTLM et Kerberos sont fournies dans la médiagraphie.

- **Principe de l'authentification**

Il est important de rappeler que la notion d' « authentification » s'applique aux objets, alors que l'identification à l'utilisateur. Lorsqu'un utilisateur se connecte sur un ordinateur relié au réseau de l'entreprise, il saisit son identifiant et mot de passe. Une requête d'authentification est envoyée à un contrôleur de domaine. En retour, le contrôleur de domaine envoie un « **Ticket Grant Ticket** », connu sous le nom de TGT, comme illustré dans la figure 4.

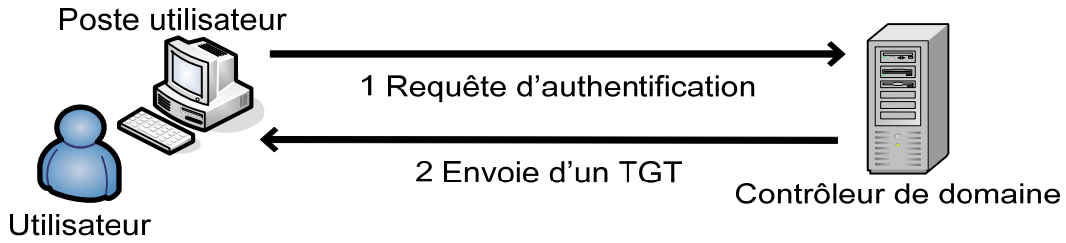


Figure 4 : Mécanisme d'authentification simplifié

- **Les API**

Les API (Application Programming Interfaces) sont des interfaces de programmation d'applications, qui permettent de connecter à l'annuaire Active directory. Ces API permettent de gérer l'active directory en utilisant différents langages de programmation.

Grâce aux API, il est possible de créer ses propres applications :

- D'administration de l'active directory : création, modification suppression des objets.
- De gestion d'accès
- Etc.

Le tableau 5 fournit les trois API les plus utilisées pour se connecter à l'active directory.

NOM de l'API	Description
API C LDAP	API LDAP est une API en langage C pour le protocole réseau LDAP.
ADSI	ADSI fournit des services et des informations Active Directory pour les applications sensibles au répertoire. ADSI prend en charge plusieurs langages de programmation, y compris Microsoft ® Visual Basic ®, C et Microsoft ® Visual C + + ®.
MAPI	Messaging API qui est pris en charge pour la compatibilité avec le client Microsoft ® Exchange et l'adresse des applications clientes du livre d'Outlook.

Tableau 5 : Liste des API, site Microsoft [18]

[18] Consultable à l'adresse http://technet.microsoft.com/en-us/library/cc961766.aspx

- **Les ports de communications**

Afin de communiquer avec l'active directory, les ports de communications sont définis selon les standard LDAP. Le choix du port de communication dépendra de la stratégie de la société en matière de sécurité.

- **Port de communication LDAP :**
  - Par défaut, les communications LDAP ne sont pas sécurisées. Le port de communication est le TCP 389.
- **Port de communication LDAPS :**
  - LDAP + Over SSL[19], est la version sécurisée du protocole LDAP. Elle utilise le port de communication TCP 636. Cette sécurisation nécessite un certificat permettant de crypter les échanges.

- **La notion de « site » dans l'active directory**

Microsoft donne la définition suivante du site : « *Un site est une partie de votre réseau où la connectivité bénéficie d'une bande passante importante et consiste, par définition, en un ensemble d'ordinateurs correctement connectés exploitant des sous-réseaux IP*», sources[20].

Le site dans l'active directory sert rediriger les requêtes d'authentification vers les contrôleurs de domaines dédiés. Il est généralement utilisé pour optimiser les temps de connexion. Le mécanisme de rattachement du site est une fonctionnalité de l'active directory et est totalement transparent pour l'utilisateur. Il se base sur l'identification du réseau (adresse IP) de l'ordinateur de l'utilisateur. Du point de vue de l'administration de l'active directory, le site permet de connaître les contrôleurs de domaine pour l'authentification de chaque sous-réseaux.

Remarque : le terme « site » désigne «le site active directory » et non «le site géographique »

Un contrôleur de domaine ne peut être rattaché qu'à un seul et unique site dans l'active directory. Si le site de rattachement couvre plusieurs régions (géographiques), les contrôleurs de domaine de ce site « desserviront » toutes ces régions. On parle alors d'« **étendu** ». Il existe deux types d'étendu.

- Etendu de sites :
  - Un site peut s'étendre sur plusieurs domaines
  - Un site peut regrouper plusieurs « régions géographiques » ou localités
  - Il peut y avoir plusieurs sites par régions
- Etendu de domaines :
  - Un domaine peut s'étendre sur plusieurs sites

Pour définir un site active directory, les informations suivantes doivent être définies, elles font références à la figure 5.

- Nom du site : (1)
- Les contrôleurs de domaines à rattacher au site : (2)
- Sous-réseaux qui seront utilisés dans le site : (3)
- Lien entre site : (4)
  - Pour chaque contrôleur de domaine il faut définir un ou plusieurs partenaires de réplication (lien). Ce partenaire peut être généré automatiquement lors de la promotion d'un serveur en tant que contrôleur de domaine. Il est possible de créer manuellement ces liens.

[19] SSL= Secure Sockets Layers, ou couche de sockets sécurisées
[20] Consultable sur : http://technet.microsoft.com/fr-fr/library/dd407869.aspx

Le schéma ci-dessous montre la console d'administration des sites et services de l'active directory.

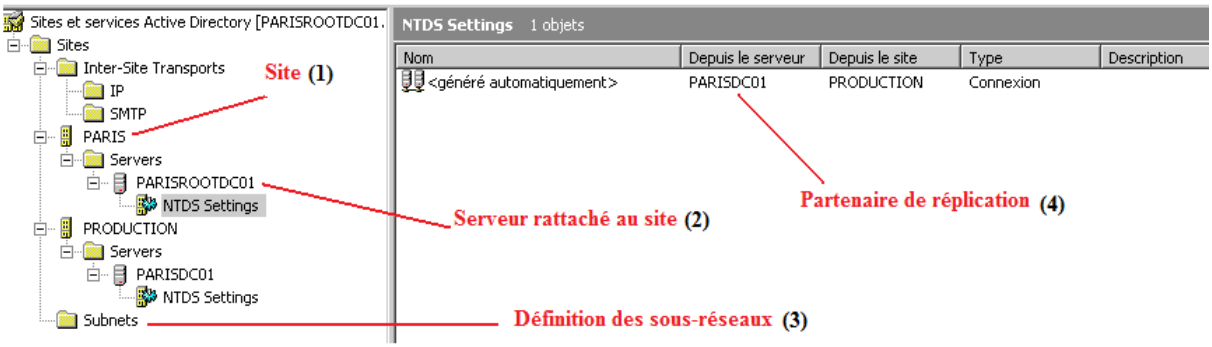


Figure 5 : Console d'administration sites et services Active Directory

Toutes ces notions sont importantes pour aborder l'architecture technique d'un active directory.

II.3.1.2 L'architecture technique de l'active directory

Deux notions sont importantes à connaître lors qu'on aborde l'architecture active directory : la notion de forêt et de schéma.
Une forêt active directory est le regroupement de plusieurs domaines partageant le même schéma, mais ne partageant pas forcément la même racine DNS ou espace de noms.
Le schéma représente la configuration commune entre les différents domaines, tel un modèle pour la création des objets. Seuls les objets du modèle peuvent être créés.

- **La forêt**

Une forêt est généralement le regroupement de plusieurs domaines au sein d'une même société. Dans certaine configuration, la forêt peut être composée d'un seul domaine (mono domaine). Cette configuration est très utilisée dans les petites structures. Dans les grandes sociétés, la configuration est généralement du type multi-domaines.
La forêt sert à hiérarchiser et organiser les domaines (active directory) de l'entreprise. L'exemple de la figure 6 montre l'arborescence de la forêt de microsoft.com. Cette représentation n'est fournie que dans le but de clarifier la notion de forêt et de domaine, sans lien direct avec l'existant chez Microsoft. Les codes couleur sont utilisés pour une meilleure lisibilité.
Dans une forêt, il y a deux notions à connaître sur les domaines

- Domaine racine ou « root domain» en anglais : **microsoft.com**
- Domaine enfant : **services.microsoft.com** et **update.microsoft.com**

Dans l'exemple de la figure 6, tous les domaines enfants partagent l'espace de nom commun «**microsoft.com**». Mais ce n'est pas toujours le cas.

Le domaine racine est le premier domaine créé dans la forêt. Il possède cinq rôles spécifiques appelés maîtres d'opérations ou « rôles FSMO[21] » décrits dans le tableau 6.

[21] FSMO : Flexible Single Master Operations

Les couleurs dans la figure 6 servent à une meilleure compréhension.

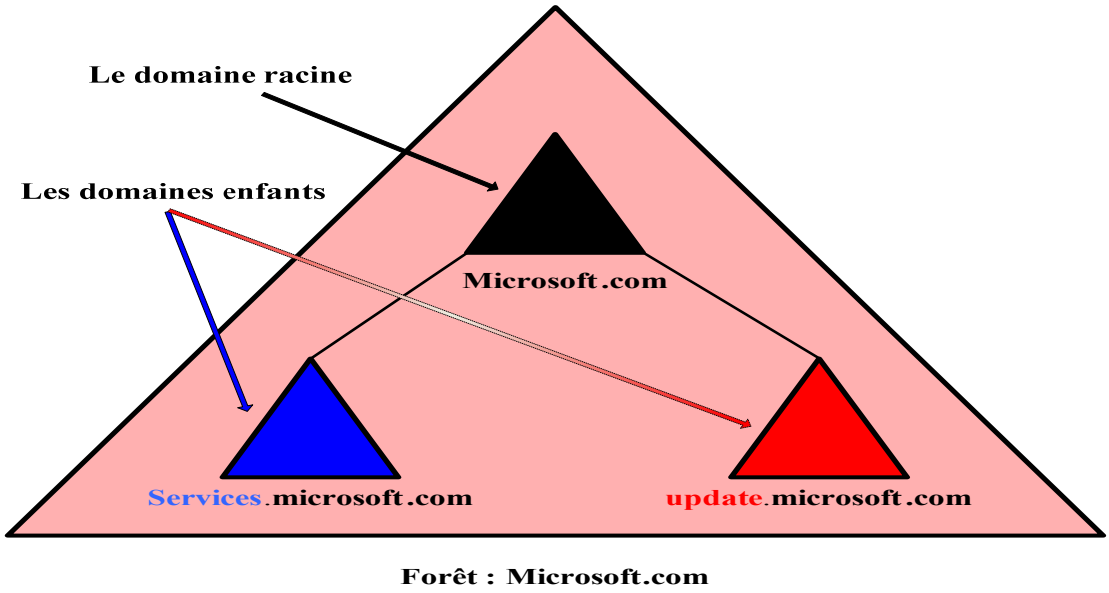


Figure 6 : Exemple de forêt active directory

- **Le schéma**

Microsoft donne la définition du schéma : « *Le schéma contient des définitions formelles de chaque classe d'objet pouvant être créée dans une forêt Active Directory. Le schéma contient également des définitions formelles de chaque attribut pouvant ou devant exister dans un objet Active Directory*. »

Cette définition n'introduit que partielle les 3 notions essentielles du schéma :

- **Les objets :**
  - Ils définissent l'ensemble des objets pouvant être créés, gérés ou stockés dans les domaines appartenant à la même forêt, voir tableau 3.
- **Les attributs :**
  - définissent les propriétés facultatives ou obligatoires de chaque objet.
    - Description, téléphone, code postal, identifiant, etc.
- **Les classes d'objets :**
  - elles regroupent les attributs liés à plusieurs objets. Les classes d'objets permettent d'éviter la redondance d'attributs.

Il est possible de modifier le schéma pour permettre l'ajout d'attributs aux objets. On parle alors d'« extension de schéma». Certaines applications nécessitent l'extension du schéma avant leur installation. C'est le cas de certaine messagerie comme Microsoft Exchange, solution de messagerie d'entreprise. Pour étendre le schéma, il faut posséder un compte appartenant au groupe : Administrateurs du schéma.
La connaissance de la composition de la forêt permet de déterminer la topologie de l'infrastructure active directory. Dans certaine littérature, on parle de « domaine racine » ou « domaine parent ». C'est dans le domaine racine et plus particulièrement sur le Maître de Schéma que ces modifications seront faites. Tous les contrôleurs de domaines de la forêt ont une copie de la configuration du schéma. La copie est synchronisée à intervalle régulier, par défaut elle est à 180 minutes.

Il est possible de modifier cette synchronisation avec une valeur minimum de 15 minutes et au maximum de 10080 minutes, soit de 15 minutes à 7 jours.

Figure 7 : Les valeurs limite de synchronisation Active Directory

Il est intéressant de comprendre l'origine des chiffres qui sont fournis. La limite des 15 minutes a été imposée afin d'éviter de saturer les réseaux en synchronisant les données de l'active directory. Cette valeur était justifiée pour les très grandes entreprises réparties dans le monde avec des sites reliés entre eux avec de faibles bandes passantes. Mais les réseaux ont beaucoup évolués depuis et les sites sont reliés entre eux par de très hauts débits.
Mais pourquoi 10080 minutes ? Cette valeur est souvent fournie sans savoir plus d'informations. C'est simplement parce que le calendrier de synchronisation pour l'active directory est de sept jours, avec la possibilité de faire une seule synchronisation par semaine.
L'active directory possède toutefois la possibilité de faire des synchronisation dite « urgente ». Cette synchronisation est déclenchée lorsque les paramètres de sécurités concernant des objets sont modifiés comme

- Le changement de mot de passe
- La désactivation d'un compte
- La suppression d'un compte
- Etc.

La figure ci-dessous illustre une synchronisation à 7 jours, soit à intervalle de 10080 minutes.

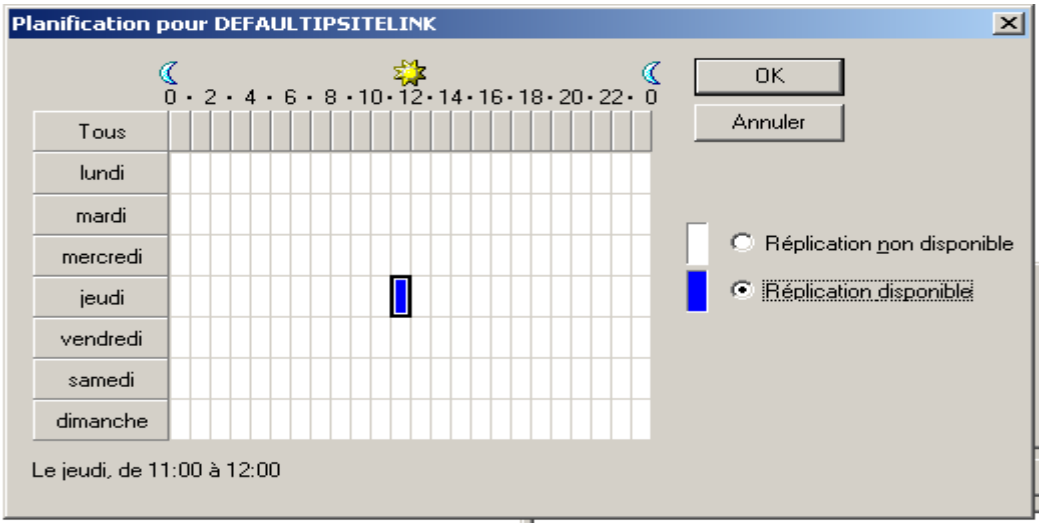


Figure 8 : Planification des synchronisations active directory

L'active directory est un annuaire synchronisé ou distribué entre l'ensemble des contrôleurs de domaines. Une politique de synchronisation supérieur à un jour n'a d'intérêt que pour les administrateurs système. Une partie de l'annuaire active directory d'une grande société non synchronisée depuis plus d'un jour « réplication obsolète » pourrait entraîner des pertes de données en cas de mauvaise synchronisation :

- pertes de toutes les modifications effectuées entre la dernière réplication et la réplication dite « réplication obsolète ».
    - perte d'objets : compte d'ordinateurs, unités d'organisation, etc.
    - perte fichiers : répertoires synchronisés, etc.
- Corruption de l'active directory
- Etc.

Le groupe AXA a mis en œuvre plusieurs active directory, afin de répondre aux exigences légales de ses propres clients. Son architecture active directory s'étend sur plusieurs régions du globe.

- **Les rôles FSMO**

Lors de la mise en place d'une infrastructure active directory, le premier serveur installé héritera automatiquement des 5 rôles de maîtres d'opérations, dites rôles FSMO (Flexible Single Master Operations en anglais).
Ces rôles seront répartis entre les contrôleurs de domaine au fur et à mesure que l'infrastructure Active directory évoluera. Il est possible de déplacer les rôles FSMO vers d'autres contrôleurs de domaines, en se référent au tableau 6.

Nom du rôle	Position	Description
Maître de schéma	1 par forêt	Le contrôleur de domaine du contrôleur de schéma contrôle toutes les mises à jour et les modifications apportées au schéma.
Maître d'attribution de noms de domaine	1 par forêt	Le contrôleur maître d'attribution de noms de domaine contrôle l'addition ou la suppression de domaines dans la forêt.
Maître d'infrastructure	1 par domaine	L'infrastructure est chargée de mettre à jour des références à partir d'objets dans son domaine aux objets dans d'autres domaines. Gère le déplacement des objets
Maître RID	1 par domaine	Le maître RID (Relative Identifier) est responsable pour un domaine particulier du traitement des requêtes de pool RID provenant de tous les contrôleurs de domaine.
Émulateur de PDC	1 par domaine	L'émulateur PDC est un contrôleur de domaine qui se proclame contrôleur principal de domaine (PDC: primary domain controller) auprès des stations de travail, des serveurs membres et des contrôleurs de domaine fonctionnant avec des versions antérieures de Windows.

Tableau 6 : Les rôles FSMO, rôles de maîtres d'opérations, source Microsoft

II.3.1.3 L'infrastructure active directory d'AXA

Le groupe AXA a depuis longtemps privilégié la redondance de son infrastructure active directory. Le cœur de l'infrastructure d'AXA est concentré sur deux data centers [22] ou centre de données en français. Ils sont situés à Lognes et à Clichy en région parisienne. Du point de vue active directory, ces deux data centers n'en forment qu'un. La seule particularité est d'avoir plusieurs sous réseaux. Il est donc possible de créer plusieurs sites pour la région Paris.
L'architecture AD d'AXA est répartie sur plusieurs sites, qui correspondent soit à des régions de France (Nantes, Paris, etc.), des DOM (La Réunion, La Guadeloupe, etc.) ou soit en sites virtuels comme la « TMA » pour Tierce Maintenance Applicative, etc.
La figure 9 est une représentation succincte d'une des architectures active directory d'AXA. Les noms des contrôleurs de domaines ont été volontairement modifiés pour des raisons de confidentialités.

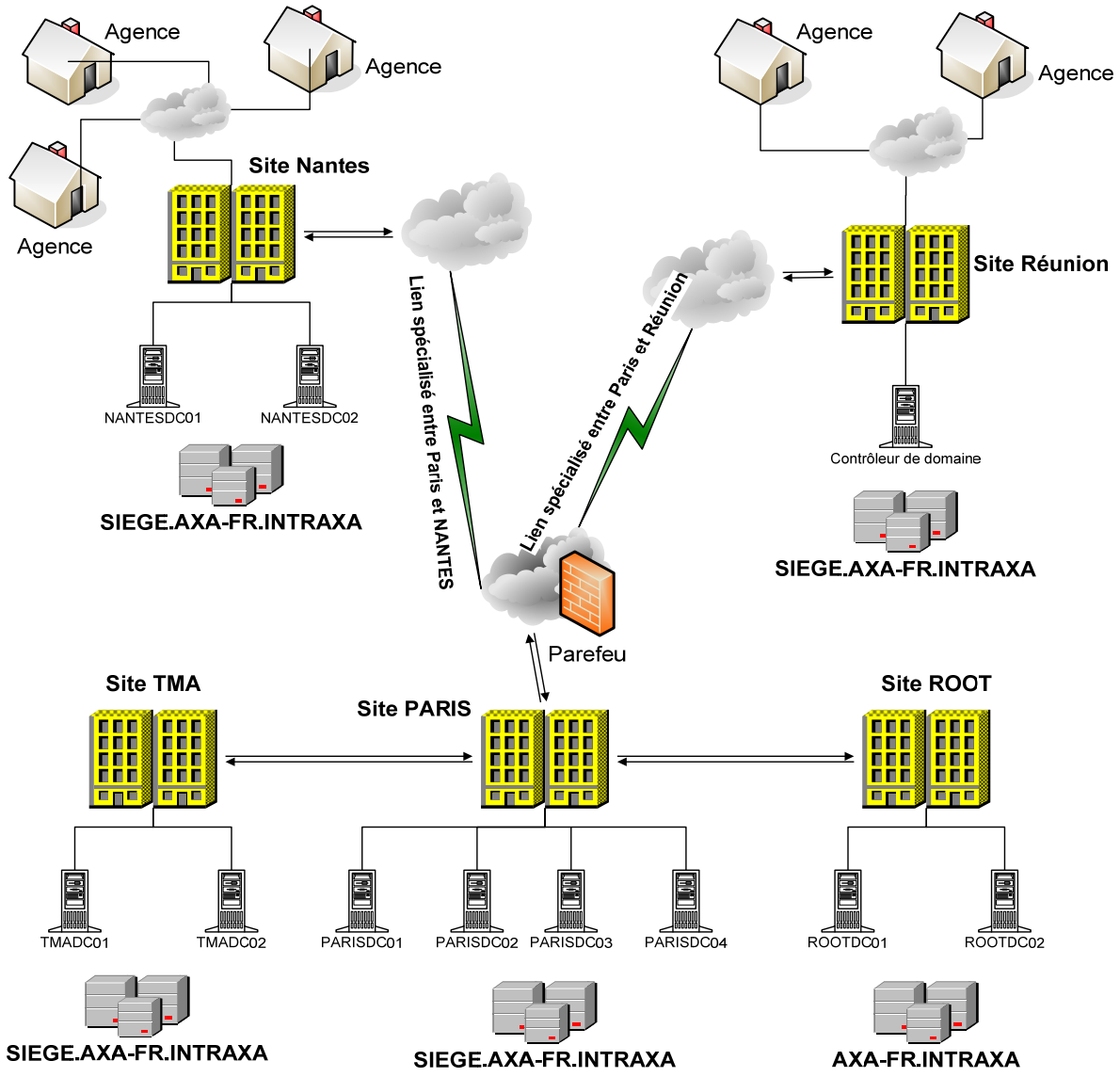


Figure 9 : Schéma de l'architecture Active directory d'AXA

[22] Data center = centre de traitement de données

II.3.1.4 Absence de tolérance de panne dans l'active directory

La multiplication des contrôleurs de domaine permet de limiter les impacts en cas de défaillance d'un des contrôleurs. Le groupe AXA possède plus d'une cinquantaine de domaines avec un minimum de deux contrôleurs pour chaque domaine. Ainsi, si un contrôleur de domaine d'un site était inaccessible, les utilisateurs dépendants de ce site auraient en théorie une chance sur deux d'être impactés. Dans les versions actuelles d'active directory, il n'y a pas de mécanisme de bascule automatique des connexions d'un contrôleur de domaine défaillant vers un autre contrôleur de domaine.
Lors de la défaillance du contrôleur de domaine nommé DC2, voir figure 10, les utilisateurs du service Marketing et du service audit interne ne pourront plus accéder à certaines ressources de l'entreprise.

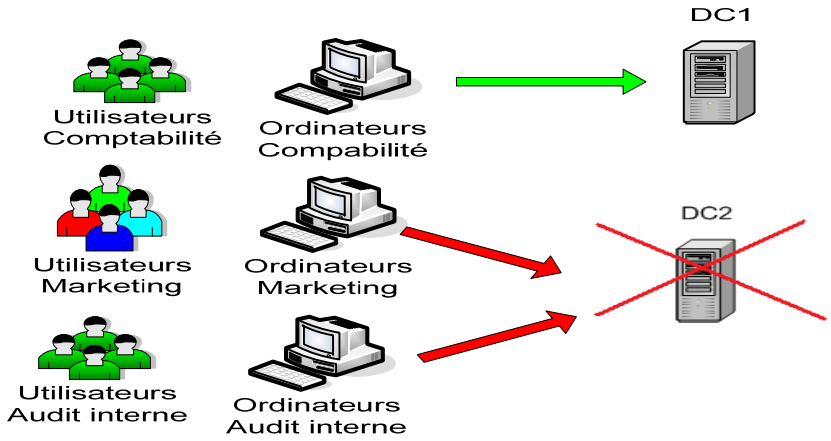


Figure 10 : Cas 1, incidents sur un contrôleur de domaine

En augmentant le nombre de contrôleurs de domaine, l'entreprise diminue la probabilité pour un utilisateur d'être affecté par un incident.
Pour palier ce problème, il est possible d'ajouter un contrôleur de domaine dans l'infrastructure, comme illustré dans la figure 11. Et ensuite affecter chaque service (comptabilité, marketing, etc.) à un contrôleur de domaine. Mais cette solution est coûteuse financièrement et en terme d'administration de l'AD.

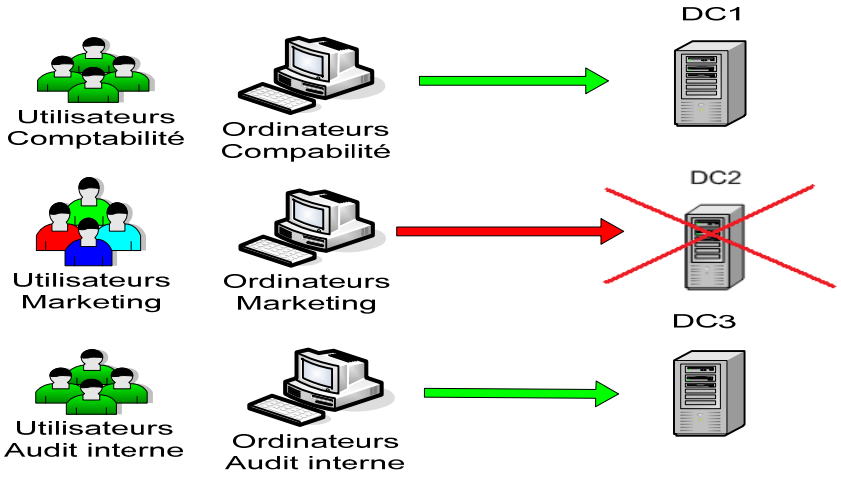


Figure 11 : Cas 2, incidents sur un contrôleur de domaine

Nous avons vu qu'il existe cinq rôles de maîtres d'opérations (les rôles FSMO, tableau 6) et ils sont uniques par domaine. La défaillance du contrôleur de domaine hébergeant un rôle empêchera toutes modifications sur l'architecture relatives à ce rôle.
Il n'y a pas de bascule automatique de ces rôles. L'éditeur Microsoft met en garde sur le transfert des rôles d'un contrôleur à un autre, et préconise les scénarios[23] suivants :

- *Le détenteur de rôle actuel est opérationnel et accessible sur le réseau par le nouveau propriétaire FSMO*
- *Vous rétrogradez gracieusement un contrôleur de domaine qui détient actuellement des rôles FSMO que vous souhaitez assigner à un contrôleur de domaine spécifique dans votre forêt Active Directory.*
- *Le contrôleur de domaine qui détient actuellement des rôles FSMO est placé hors connexion pour des opérations de maintenance planifiées et certains rôles FSMO spécifiques doivent être assignés à un contrôleur de domaine « live »(en ligne). Cela peut être requis pour effectuer des opérations qui assurent une connexion au propriétaire FSMO. Cela serait particulièrement vrai pour le rôle d'émulateur PDC, mais moins vrai pour le rôle de maître RID, le rôle de maître d'opérations des noms de domaine et le rôle de contrôleur de schéma. (sources Microsof.fr)*

La figure ci-dessous montre la répartition des rôles FSMO dans une forêt active directory.

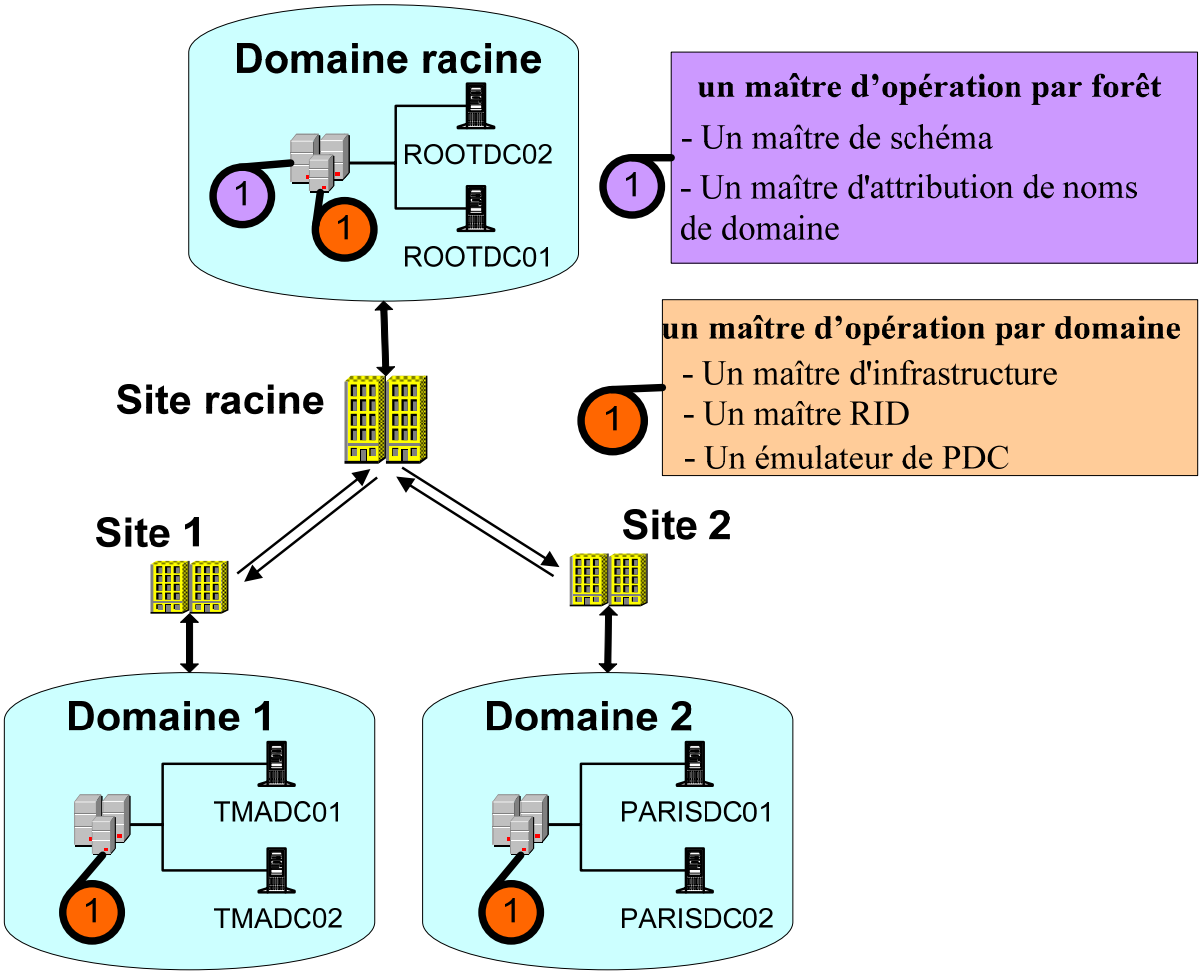


Figure 12 : La répartition des rôles FSMO

[23] http://support.microsoft.com/kb/255504/fr

En l'absence d'une réelle solution de tolérance de panne intégrée à l'active directory, de nombreux incidents sur des contrôleurs de domaines du groupe AXA ont fortement perturbé l'activité du groupe. Les incidents sur des contrôleurs de domaines des sites principaux (Clichy et Lognes) ont perturbé le fonctionnement de tout le groupe AXA :

- Messagerie
- Accès Internet
- Applications majeures
- Accès aux fichiers partagés
- Etc.

Des incidents à répétition d'une telle envergure sur l'annuaire de l'entreprise ont affecté la confiance des utilisateurs et de la direction du groupe.

La surveillance de l'active directory doit être mise en place afin d'être réactif et limiter les conséquences.

II.3.1.5 La surveillance de l'active directory (AD)

La connaissance de l'environnement AD permet de cibler les éléments à superviser. Les outils de supervision du marché intègrent des fonctionnalités de surveillance de l'active directory. L'outil de supervision utilisé par AXA, la solution de Computer Associates, CA NSM[24] 3.1 ne permet pas de superviser l'active directory.

L'éditeur Computeur Associates (CA), propose depuis 2009 la version NSM r11 qui prend en charge l'active directory : NSM r11 Active Directory Management Option. La qualification de cette version était en cours lors du lancement du projet de la supervision de l'active directory.

L'étude des différents incidents rencontrés durant plusieurs mois m'a permis d'affiner les éléments critiques de l'active directory à surveiller. La gestion des incidents dans une base centralisée référençant tous les incidents d'AXA a facilité cette recherche.

Les cinq points suivants ont été identifiés lors de l'analyse des incidents comme générateur de plus d'incidents sur les contrôleurs de domaine :

- L'authentification des comptes (utilisateurs ou ordinateurs) : Ce mécanisme permet de s'assurer que le couple « compte/mot de passe » est valide. L'authentification est indispensable pour accéder à certaines ressources de l'entreprise. Le test devra vérifier que le serveur valide deux comptes de tests créés spécifiquement pour le projet. Si au moins un des deux comptes est validé, le test sera considéré comme satisfaisant aux résultats attendus.

- Les réponses DNS (Domain Name System en anglais) ou Système de Nom de Domaine : permettent de traduire un nom de domaine en plusieurs types d'informations, tel que l'adresse IP de la machine portant ce nom de domaine. La résolution des noms de domaines est nécessaire pour accéder aux ressources internes ou extérieures de la société. Le test consistera à interroger le serveur DNS sur la zone DNS qu'il héberge.

- Le test de présence d'enregistrements critiques dans le DNS est basé sur le même principe que les réponses DNS. Ce sont des enregistrements DNS qui permettent d'accéder à des ressources de l'entreprise. Le test consistera à interroger un DNS de l'active directory pour s'assurer que les enregistrements sont bien présents.

[24] NSM : Network and systems management

- Les services Windows : Sur un contrôleur de domaine, certains services sont nécessaires pour le bon fonctionnement de l'active directory. Ces services doivent être démarrés afin de remplir leur rôle. Ils permettent de répondre aux requêtes des utilisateurs, des ordinateurs ou toutes les applications sur le réseau de l'entreprise. Seuls l'état des services seront pris en compte : démarré, arrêté, etc.

- Compte d'installation des serveurs : Ce compte sert à l'installation automatisée des serveurs. En cas de disfonctionnement, c'est toute la chaîne d'industrialisation qui serait bloquée. La chaîne doit être débloquée manuellement par un superviseur d'installation.
  Il faut s'assurer que ce compte soit opérationnel, qu'il ne soit pas verrouillé, où que le mot de passe n'a pas été changé. Ce test est basé sur le test « authentification des comptes ».

Les éléments importants, mais non indispensable au fonctionnement de l'active directory ne seront pas supervisés. Ils seront supervisés par l'outil de supervision CA NSM 3.1.

II.3.2 Les bases de la supervision informatique

La supervision informatique est un mécanisme qui test ou contrôle le fonctionnement d'un système. Elle permet d'alerter les équipes exploitantes lors de l'apparition d'une anomalie sur l'infrastructure informatique. Il existe deux types de supervision :

- Supervision avec un agent
  - Un agent est un logiciel installé sur l'équipement à superviser
  - Quand une anomalie est détectée, l'agent la remonte à la supervision centrale, qui se charge d'alerter par les équipes concernées.
- Supervision sans agent
  - Il n'y a pas d'installation de logiciel client sur le serveur à superviser

Le principe de la supervision est repris dans la figure 13. Il existe plusieurs modèles, mais celui présenté est le plus courant.

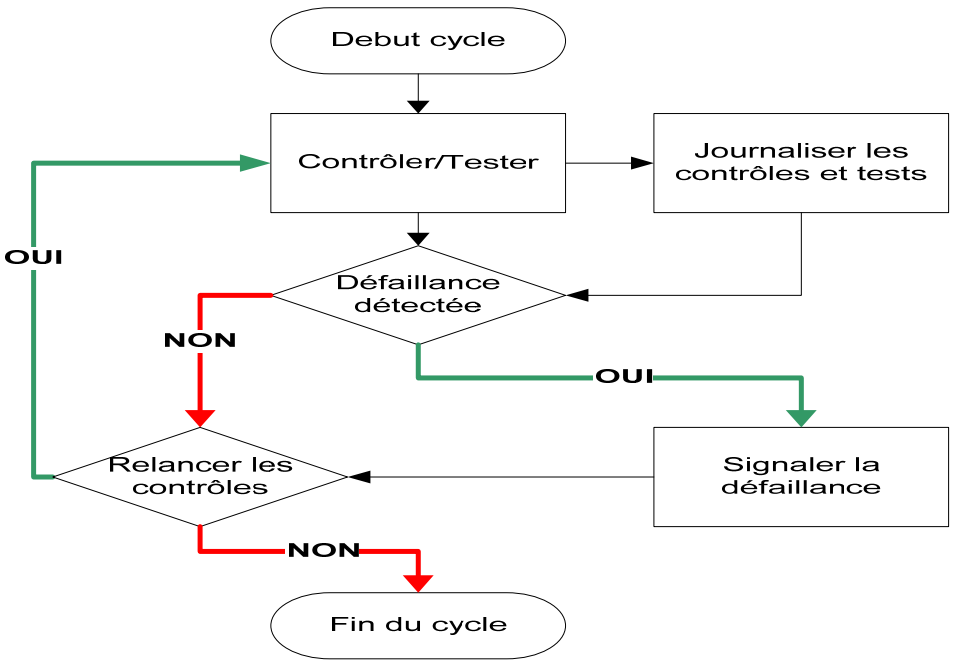


Figure 13 : Diagramme simplifié de supervision.

II.3.3 La supervision avec et sans agents

Les activités des entreprises ont beaucoup évolué. Le système d'information fonctionne sans interruption. La supervision avec un agent nécessite l'installation d'un logiciel client sur le serveur à superviser. AXA interdit l'installation de composants ou logiciels sur des serveurs de production pendant les plages de production.
Sur de vastes infrastructures comme AXA, l'installation des agents peut nécessiter des ressources importantes. Dans ce cas, l'installation des agents doit faire l'objet d'un projet.
La supervision sans agent ne nécessite pas de composants supplémentaires sur le serveur à superviser. Elle est facile à déployer sur de vastes infrastructures.
La supervision sans agent sera recommandée pour des infrastructures de taille modeste. La supervision avec un agent sera utilisée lorsque les performances seront nécessaires.

II.3.3.1 La supervision avec agent

La supervision avec un agent nécessite l'installation d'un logiciel client sur le serveur à superviser. Le déploiement d'une telle supervision est un projet a lui seul.
Chaque agent installé doit être configuré sur chaque serveur. Une configuration de base peut être déployée sur l'ensemble des serveurs à superviser. Les configurations spécifiques seront ensuite appliquées selon plusieurs modèles :

- En regroupant les serveurs ayant les mêmes caractéristiques techniques
  - Nécessite une gestion rigoureuse des configurations
- En appliquant une configuration spécifique pour chaque serveur
  - Long et fastidieux
- L'auto-découverte
  - L'agent de supervision installé détecte automatiquement les caractéristiques du serveur à superviser.
- Etc.

- **Fonctionnement**

La supervision avec agent est généralement composée d'un ou plusieurs collecteurs. Les collecteurs communiquent avec les agents installés sur les serveurs à superviser. Les résultats des tests de supervision sont sauvegardés dans une base de données. Ces données sont utilisées afin d'alimenter la cartographie ou la « MAP ».

L'architecture d'une supervision avec agent est composée :

- D'une base de données
  - Les données collectées sur les serveurs supervisés
  - La configuration des agents
  - La configuration des collecteurs
  - Les données de performance
  - Etc.

- De collecteurs : ils sont chargés récupérer les informations collectées lors des tests par les agents installés sur les serveurs à superviser
- D'une console centrale d'administration
- Une cartographie des serveurs supervisés
- Etc.

La figure 14 est un exemple d'architecture de supervision avec agent.

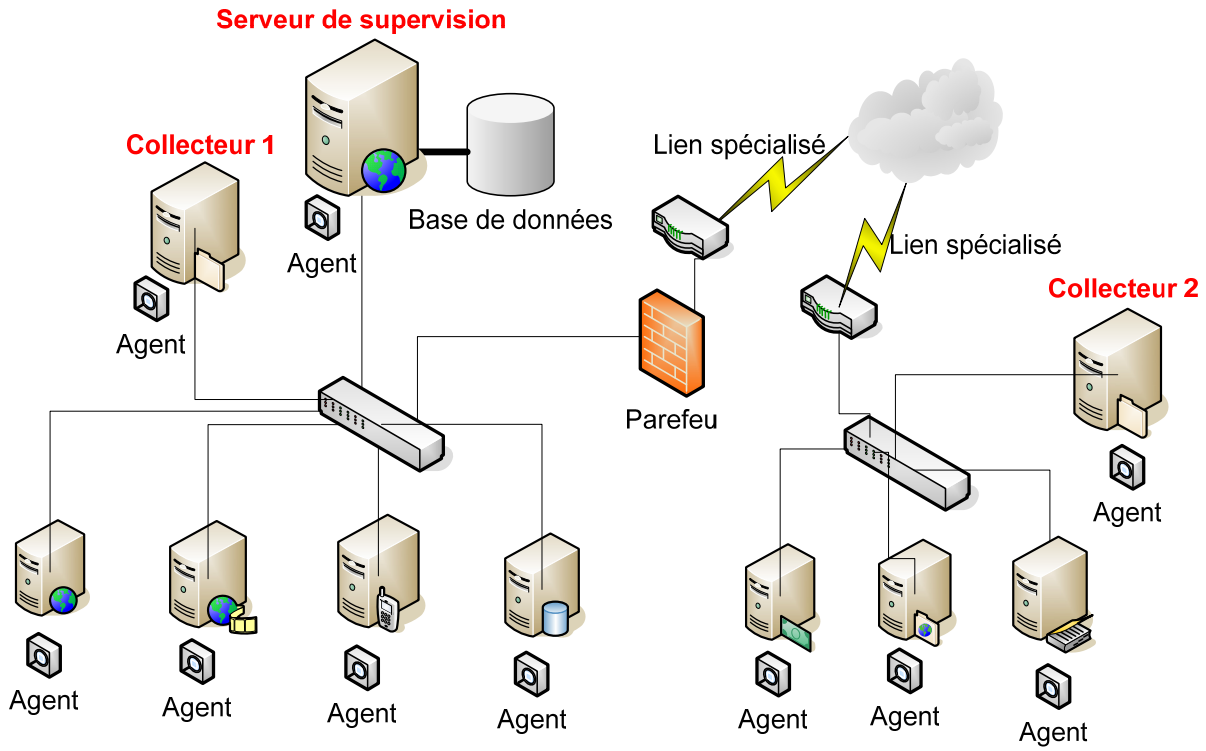


Figure 14 : Exemple d'architecture de supervision avec agent

Le déploiement de l'agent peut mobiliser des ressources de l'entreprise et nécessite des outils de déploiement pour les volumes importants de serveurs.

II.3.3.2 La supervision sans agent

La supervision sans agent ne nécessite pas d'installation sur le serveur à superviser. Les risques liés à l'installation de composants sur des serveurs en productions sont limités. La supervision sans agent permet une mise en production rapide des serveurs à superviser. Son déploiement est piloté depuis la console de supervision. Les serveurs à superviser sont créés directement dans la console de gestion de la supervision centrale.
La liste des serveurs à superviser peut être créée en utilisant un fichier modèle au format « .CSV » (Comma-Separated Values), ou « valeurs séparées par des virgules » en français.
La supervision sans agent peut utiliser des technologies différentes pour fonctionner sur le serveur à superviser :

- SNMP : Simple Network Management Protocole
  - protocole de communication pour l'administration et la supervision des équipements réseaux
- WMI : Windows Management Instrumentation
  - Infrastructure de gestion de Windows
- Etc.

La supervision de systèmes informatiques doit être intégrée dans la gestion du risque opérationnel de la société. Elle doit être valorisée comme un investissement à long terme.

II.3.3.3 Evaluation de la supervision

L'architecture de supervision est un maillon essentiel dans la gestion du risque au sein de l'entreprise. Une étude comparative des différents systèmes de supervision donnera les lignes directrices pour la DSI.
L'évaluation des outils de supervision ne doit pas s'arrêter à l'étude comparative des coûts les plus bas. Elle doit permettre d'évaluer aussi les risques liés à la sécurité, s'inscrire comme un investissement à long terme et doit prendre en compte l'évolution des systèmes.
Le tableau 7 est un comparatif de la supervision avec et sans agent. Il permet d'évaluer le type d'architecture à mettre place.

Supervision avec agent	Supervision sans agent
Déploiement long et fastidieux	Déploiement rapide et facile
Nécessite plus de ressources	Mobilise moins de ressources
Système réactif et performant	Dépend de la taille de l'architecture
Supervision étendue à tous les composants du système	Supervision limitée à certains composants du système
Sécurité renforcée	Risque potentiel de sécurité
Augmentation du trafic réseau	Trafic réseau réduit
Mise à jour de l'agent fastidieux	Pas d'agent
Evolution complexe	Evolution facile
Coût global important	Coût global plus faible

Point faible
Point fort

Tableau 7 : La supervision avec et sans agent

II.3.3.4 La supervision CA NSM 3.1

ATS utilise l'outil de supervision NSM 3.1 de la société Computer Associates (CA). NSM permet de superviser des systèmes d'exploitation hétérogènes.
La supervision NSM est une supervision avec agent. Le principe de fonctionnement de la supervision avec agent est présenté dans la section II.3.3.1. Les collecteurs NSM sont appelés DSM pour « Distributed State Machine », ou Machine à états distribués en français.
La supervision NSM 3.1 a permis de répondre aux exigences des DSI durant des années. Elle permet de superviser un grand nombre de composants des systèmes d'informations, tels que :

- Les services du système d'exploitation
- Les espaces disques : dépassement de seuils d'espaces disques
- Les événements du système
- Les performances du système
- Les fichiers d'échanges du système
- Les bases de données (nécessitent un agent spécial)
- Les interfaces réseaux : l'état des interfaces réseaux
- Les clusters (partages de ressources entre plusieurs serveurs)
- Etc.

NSM 3.1 est un outil de supervision dédié aux entreprises. Il a été conçu pour répondre aux exigences des DSI dans le domaine de la supervision.

- **Les performances de CA NSM**

Les performances de la supervision CA NSM sont renforcées grâce aux agents installés sur les systèmes à superviser. Une bonne répartition des DSM[25] dans l'architecture permet d'accroître considérablement les performances de la supervision.
L'évaluation des performances de la supervision est réalisée avec l'agent de performance, un sous-système de la supervision. L'agent de performance CA NSM fournit des événements liés aux performances d'un large éventail de systèmes d'exploitation.
Les performances de la supervision dépendent d'un certain nombre paramètres :

- La taille et la conception de l'architecture de supervision
- De la stratégie de supervision : le nombre d'éléments supervisés
- Des performances du système supervisé
- Etc.

- **Les points faibles de CA NSM3.1**

La supervision NSM impose que l'agent NSM soit connecté en permanence au serveur DSM. Ces nombreux échanges avec le DSM sont consommateurs de bandes passantes, c'est-à-dire qu'il y a une augmentation du trafic réseau.
Dans certaine architecture réseau ayant de faibles bandes passantes entre le site central et les sites secondaires, l'utilisation de serveurs DSM est nécessaire pour améliorer les performances de la supervision.
Le groupe AXA a fait le choix de ne pas superviser les serveurs se trouvant sur des sites secondaires avec la solution CA NSM. Les coûts seraient trop élevés. Il faudrait autant de DSM supplémentaires que de sites. Chaque DSM ne superviserait en moyenne que 2 à 3 serveurs au maximum.

- **Le cycle de vie de CA NSM 3.1**

Les systèmes d'exploitation ont beaucoup évolué, et la solution NSM 3.1 est devenue obsolète. Créée en 2004, elle est arrivée en fin de cycle de vie. Computer Associates propose désormais une nouvelle version NSM r11, avec en option la supervision de l'active directory, qui faisait défaut dans la version NSM 3.1.

- **Etat des lieux chez ATS**

Une étude a été menée courant 2012 en vu de remplacer le produit CA NSM 3.1 par des solutions de supervision dans le domaine libre (open source linux). J'ai participé à cette étude en tant que consultant. Mais ce projet n'a abouti, car il était trop coûteux. De nombreux développements avaient été faits autour de CA NSM.
Un projet est en cours chez ATS afin de migrer la version NSM3.1 vers NSM r11. Aujourd'hui, une architecture NSM r11 est installée, elle était jusqu'ici en cours de validation opérationnelle.

[25] DSM : « Distributed State Machine », ou Machine à états distribués en français

II.3.4 La supervision et les interactions avec le système supervisé

La supervision informatique est aujourd'hui indispensable dans les grandes sociétés. Avec des centaines ou des milliers de serveurs à administrer, et plusieurs points de contrôles par serveurs, l'automatisation de ces contrôles devient nécessaire. La supervision automatise ces points de contrôles.
Le système de supervision peut être utilisé pour interagir avec le système à surveiller. Cette supervision avec interaction, dite proactive, tente de corriger les anomalies dès leur apparition.
La supervision sans interaction, dite passive, ne sert qu'à alerter sans modification sur le système à surveiller.
Le choix de la supervision doit s'inscrire dans la politique à long terme de la direction du système d'information (DSI).

II.3.4.1 La supervision avec ou sans interactions

- **La supervision avec interaction**

La supervision avec interaction ou « proactive » agit directement sur les systèmes supervisés en appliquant des scénarios de correction des incidents. Ceci réduit considérablement le nombre d'incidents à traiter par les équipes exploitantes. Le retour d'expérience sur les différentes anomalies rencontrées facilite la mise en place des correctifs. Ainsi, un service du système d'exploitation qui est arrêté, sera démarré par l'outil de supervision, sans qu'aucun exploitant n'intervienne. Toutefois, le service exploitant pourra être informé de cet incident.
Il est alors possible de mettre en place un scénario de correction pour chaque anomalie. Les scénarios sont définis par les équipes techniques.
La supervision avec interaction nécessite une bonne maîtrise des environnements supervisés. La mise en place des scénarios doit être maîtrisée. Ces scénarios sont formalisés par des scripts, des « batches » ou des lignes de commandes qui seront exécutés sur le serveur supervisé.
Quand certaines anomalies nécessitent l'intervention des équipes techniques, ils seront alertés par la supervision.
Les équipes d'exploitation se concentrent sur les activités les plus complexes et dont la valeur ajoutée est plus importante. Leur travail est ainsi valorisé.

- **La supervision sans interaction**

La fonction de base de la supervision, est la surveillance sans interaction. Cette supervision dite « passive » n'agit pas sur le système à surveiller. Les incidents sont remontés par la supervision et persisteront jusqu'à ce que les équipes d'exploitation les résolvent.
Les équipes de pilotage ou de « pupitre » sont chargées de contrôler les différents incidents remontés par la supervision. Elles appliquent les consignes ou procédures en vu de résoudre ces incidents. Ces opérateurs sont le plus souvent le premier niveau support. Avec des procédures pour chaque serveur, ils traitent une très grande majorité des incidents. Ces procédures permettent de déléguer la gestion des incidents à des opérateurs ne nécessitant pas forcément de très bonnes compétences techniques.
Le nombre d'alertes peut vite croître si les opérateurs ne sont pas réactifs. Cette supervision nécessite plus de ressources humaines pour la gestion des incidents. Le sentiment de faire un travail répétitif et non valorisant est fort.

II.3.4.2 Choisir sa supervision

La DSI doit inscrire dans sa politique de gouvernance le type de supervision à mettre en place. Elle doit imposer ses contraintes en se basant sur le retour d'expérience.
Le choix de la supervision nécessite de prendre en compte les ressources disponibles dans l'entreprise pour traiter l'ensemble des alertes.
Le tableau 8 est une étude comparative que j'ai faite sur la supervision avec et sans interaction.

Supervision avec interaction	Supervision sans interaction
alertes	Alertes
Réactivité grâce aux scénarios de corrections	Dépend de la réactivité des équipes
Réduction du nombre d'incidents à traiter	Incidents plus nombreux
Valorisation du travail	Nécessite plus d'opérateurs
Traçabilité des actions est faible	Recherche de solutions pérennes
Réduction des effectifs	Externalisation fréquente

Point fort
Point faible
neutre

Tableau 8 : Comparaison de la supervision avec et sans interaction

II.3.5 Planification de la supervision

La supervision informatique est un ensemble de tests et contrôles continus sur les équipements informatiques. La fréquence de ces contrôles varie selon le type de supervision à mettre en œuvre : avec ou sans agent.
Les agents de supervision installés sur les serveurs se connectent à des collecteurs (relais de supervision) ou à la supervision centrale. Les vérifications et tests sont faits en continue par l'agent installé. Dès l'apparition d'une anomalie, l'agent remonte immédiatement cette anomalie à son serveur relais ou à la supervision centrale.
Dans le cas d'une supervision sans agent, ce sont les relais de supervision et la supervision centrale qui planifient les contrôles. Il peut se passer plusieurs minutes avant que la supervision centrale ne détecte l'apparition d'une anomalie.
La supervision sans agent nécessite un planificateur de taches afin de répéter les contrôles. Les solutions de supervision du marché ont un « planificateur de taches » intégré. Dans le cadre du projet, j'utiliserai un ordonnanceur qui joue le rôle de planificateur de tâches. L'ordonnanceur utilisé par AXA est IBM Tivoli Workload Scheduler (TWS). Les agents TWS sont présents sur tous les serveurs d'AXA. Ils seront intégrés dans la conception de la supervision.
L'étude de l'ordonnanceur est nécessaire pour comprendre le fonctionnement de la supervision. Il fait parti du cœur de la supervision qui sera mis en place.

II.4 L'étude de ordonnanceur Tivoli Workload Scheduler (TWS) d'IBM

Les applications informatiques utilisent de plus en plus des chaînes de traitements de données ou WorkFlow en anglais. La coordination de ces chaînes de traitement favorise l'automatisation de l'information et des données. Elles peuvent provenir d'applications ou plateformes hétérogènes.
Les entreprises qui réalisent beaucoup de traitements ont besoin de centraliser la gestion de ces flux. Les séquences doivent être maîtrisées tout au long de la chaîne et stoppées si besoin.
L'ordonnanceur TWS répond à ces contraintes. Il permet de planifier ces taches et de créer des dépendances entre les différentes taches.
TWS est bien plus qu'un planificateur de taches Windows. Il permet de hiérarchiser les taches, en positionnant des points critiques dans la chaîne. Ces points critiques permettent de stopper la chaîne en cas d'erreur de traitement.

II.4.1 Généralités et principe de fonctionnement

TWS est un outil d'automatisation, de surveillance et de contrôle des travaux et des flux de travaux. Son intégration dans l'entreprise permet de gérer des flux de traitements importants tout en alliant la performance et la flexibilité. Il participe à la réduction des coûts en offrant un point unique de contrôle et d'administration des travaux.
TWS est basé sur des normes ouvertes permettant d'être interfacé avec d'autres solutions du marché. Les développements autour de TWS sont ainsi pérennes et évolutifs.
Il permet le traitement des travaux des systèmes d'exploitation hétérogène : Linux, Unix, Microsoft Windows, etc.
TWS est une application installée sur un serveur Mainframe qui a une grande puissance de calculs. Le système d'exploitation utilisé sur le Mainframe est le Z/OS d'IBM apparu dans sa version initiale dans les années 1960.
Deux notions fondamentales sont à connaître lors de l'étude de l'ordonnanceur TWS :

- La base de données
  - Contient toutes les définitions des objets dans TWS
- Le plan
  - Contient les traitements à exécuter dans les 24h

II.4.1.1 Les travaux et flux de travaux

Du point de vu d'un ordonnanceur, les travaux ou jobs (en anglais) sont des unités de temps réservées pour exécuter des traitements sur un système. Ces traitements peuvent être l'exécution de scripts, d'exécutables, de commandes, etc.
Les travaux ou jobs comportent les caractéristiques suivantes :

- Nom du traitement
- Non de la station de travail (client TWS)
- Nombre de traitements simultanés
- La priorité du traitement
- L'environnement : production, pré-production, développement, etc.
- Programmes à exécuter
- Etc.

Les flux de travaux ou jobstream (en anglais) sont des enchaînements de travaux liés entre eux par des dépendances. Il y a plusieurs types de dépendances : horaire, prédécesseurs, reprises sur incidents, etc.
Les flux de travaux peuvent contenir des travaux se trouvant sur des systèmes d'exploitation différents. Ils permettent d'automatiser et de contrôler le déroulement des traitements. Des scénarios sont possibles pour limiter les interventions des équipes exploitantes sur la chaîne de traitement.
Les travaux ayant des dépendances peuvent interrompre toute la chaîne en cas d'erreur. Mais il est possible de laisser se poursuivre la chaîne de traitements en cas d'erreur. Dans la figure 15, en cas d'échec sur les travaux **N3**, les travaux suivants ne seront pas exécutés : **N4** et **N5**. Car le job N3 est un point critique de la chaine.

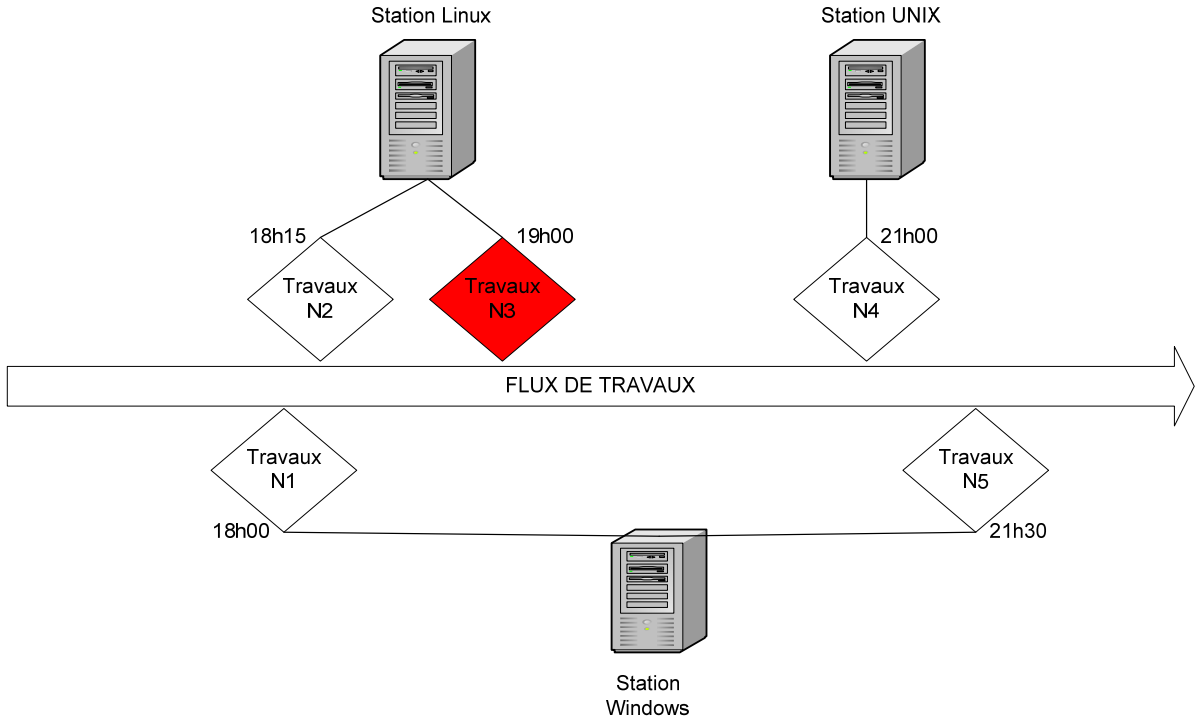


Figure 15 : Flux de travaux dans TWS

II.4.1.2 La base de données de l'ordonnanceur

La société IBM, l'éditeur de TWS, fournit en standard son système de gestion de base de données (SGBD) connu sous le nom de BD2 (Data Base2). DB2 est un système propriétaire d'IBM. L'ordonnanceur TWS est aussi compatible avec le SGBD l'éditeur Oracle (base oracle).
La base de données de TWS comporte les informations suivantes :

- Les définitions d'objet de base fournies par l'éditeur
- Les travaux et flux de travaux
- Définition des travaux
- Les postes de travail ou stations (serveurs)
- L'identifiant des comptes de services, mot de passe et domaine d'appartenance
- Etc.

Pour les domaines multiples avec des comptes de service identiques, les travaux doivent être associés au compte de service ayant les autorisations suffisantes sur la station de travail.
La base de données permet de consulter l'ensemble des travaux à venir et de modifier leur planification. La gestion centralisée de plusieurs environnements de travail, est possible en créant des bases distinctes :

- Base de production
- Base d'homologation
- Base de recette
- etc.

Les audits peuvent être activés afin de tracer les opérations effectuées par les utilisateurs.

II.4.1.3 La notion de plan dans TWS

Les travaux à exécuter dans les prochaines 24h sont extraits de la base de données pour constituer le plan courant. Le plan courant est généré tous les jours à heure fixe. Par défaut, il est à 06h00. On parle alors de la montée au plan courant. Chez AXA, la montée au plan est à 10h00, heure à laquelle les travaux sont les moins nombreux.
Un plan contient :

- Les dépendances entre les différents travaux
- Les travaux à réaliser sur 24h
- Les travaux en cours ou terminés
- Etc.

Les travaux qui ne sont pas dans le plan courant peuvent être montés au plan. On parle alors de « **forcer la montée au plan** ». Cette montée au plan forcée permet d'exécuter des traitements immédiatement ou des traitements différés dans le plan en cours.
Selon les politiques de l'entreprise, la modification du plan courant ne sera possible que dans certains environnements : développement, recette, etc.
La politique d'AXA n'autorise la modification du plan courant que par les équipes d'administration de la plateforme d'ordonnancement, et non pas par les équipes exploitantes. Alors que les autres environnements sont ouverts à la modification du plan courant par toutes les équipes.

II.4.2 Contraintes de l'ordonnanceur

L'utilisation d'un ordonnanceur nécessite de prendre en compte quelques contraintes. L'ordonnanceur utilise les codes retour d'exécution des scripts et des programmes afin d'affiner les scénarios définis par les exploitants.
Les stations de travail, clients de l'ordonnanceur, doivent remplir des conditions indispensables pour l'exécution des traitements.

II.4.2.1 Les contraintes liés aux scripts et programmes

Lors de l'exécution d'un script, il se termine avec un code de fin d'exécution. Ce code numérique est appelé code retour. Si tout se passe bien, le code retour est 0 (zéro). Toute valeur supérieure à 0 signale qu'une anomalie a été détectée.

Dans l'environnement Windows, la variable contenant le code retour s'appelle «**errorlevel**». Pour accéder au contenu du code retour, on utilise : **%errorlevel**%.

Ce code retour d'exécution des batches ou script peut être modifié afin de changer les scénarios de l'ordonnanceur. Le script peut être modifié afin que les travaux en erreur retour une code retour « 0 », correspondant à une opération réussie. La commande « **set errorlevel=0**», placée en fin du script à exécuter permet de forcer le code retour à 0.
Il convient d'être prudent lors des modifications de ces codes retour. La gestion des erreurs par l'ordonnanceur peut être inhibée et les traitements en erreurs peuvent avoir de lourdes conséquences pour la production.
Le tableau 9 donne quelques exemples de codes retour et la description associée.

Code retour	**Description de la valeur**
0	Opération réussie.
1	erreur d'argument
13	Données non valides.
87	L'un des paramètres n'est pas correct.
100	Pas assez de mémoire.

Tableau 9 : Exemples de codes retour

II.4.2.2 Les contraintes liés aux stations de travail

Les stations connectées à l'ordonnanceur doivent être conformes aux exigences suivantes :

- La synchronisation de l'horloge entre les stations et l'ordonnanceur
  - L'horloge de l'ordonnanceur et de la station doivent être identique.

- La résolution des noms de toutes les stations depuis l'ordonnanceur
  - L'ordonnanceur doit pouvoir associer le nom de la station à son adresse IP

- Les comptes d'exécution des traitements ont les droits suffisants sur les stations
  - Un compte de service dédié à l'exécution des travaux doit avoir les privilèges nécessaires sur les stations
  - Compte local ou compte du domaine

- Les stations de travail sont accessibles depuis l'ordonnanceur
  - Les stations qui se trouvent dans zone réseaux avec des systèmes de protection, doivent être accessibles par l'ordonnanceur.
  - Des règles de filtrage sont nécessaires sur les pare-feux.

- Les programmes et les scripts doivent être présents sur les stations
  - Les scripts et programmes nécessaires pour le traitement des travaux doivent être au préalable présents.
  - Le programme client (ou agent) de l'ordonnanceur doit être en cours d'exécution sur la station.

D'autres contraintes peuvent être imposées en fonctions des politiques internes de chaque société.

II.4.3 L'architecture de l'ordonnanceur d'AXA

L'ordonnanceur a pris une place de plus en plus importante dans le traitement de l'information.
Il est devenue aujourd'hui incontournable dans certaine société tant le nombre de traitements est important. Les sociétés se dotent le plus souvent d'architecture d'ordonnanceur redondée. Cette architecture active/passive permet la tolérance de panne. AXA a opté pour la solution de redondance en utilisant deux serveurs mainframes dédiés à l'ordonnancement. Ils sont répartis sur deux sites en région parisienne : à Lognes et à Clichy.
Les bases de données des différents environnements sont répliquées entre les deux serveurs. Pour chaque environnement, il n'y a qu'une base de données active à la fois, elle est notée « **Maître** », sur la figure 16.

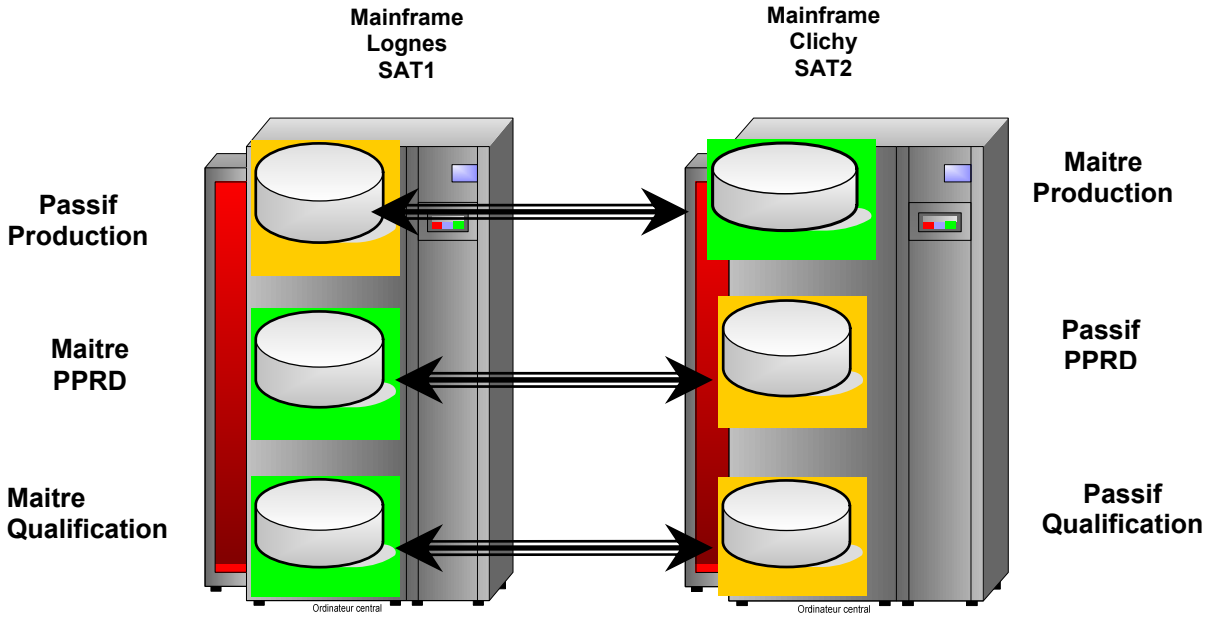


Figure 16 : Architecture mainframe AXA Tech

II.4.3.1 Architecture matérielle

L'architecture matérielle des ordonnanceurs est composée de serveurs ayant une grande puissance de calculs. Le choix de la plateforme matérielle dépend du nombre de traitements à exécuter et des stratégies de l'entreprise. Les solutions proposées par IBM ont depuis des décennies faites leur preuve dans les grandes sociétés.
Le groupe AXA a opté pour deux modèles 2097 d'IBM dont les caractéristiques sont fournies ci-dessous.

- Type de machine : Z10
- Modèle : E12 (2097-706 et 2097-709)
- 6 et 9 processeurs
- 96 Go de RAM pour chaque serveur Z10

Les caractéristiques techniques sont fournies dans les tableaux 10 et 11.

La figure 17 est une photo du system Z10 d'IBM, aux dimensions impressionnantes

Figure 17 : Photo de l'IBM System Z10

La gamme Z10 se décline en 5 modèles. Les deux derniers chiffres numéros du modèle 2097-7XX indiquent le nombre de processeurs commandés par le client. Pour les appellations EXX, les deux derniers chiffres indiquent la taille maximum de mémoire pouvant être installée.

Mémoire processeur

Modèle	Minimum	Maximum[7]
E12	16 Go	384[8] Go
E26	16 Go	752 Go
E40	16 Go	1136 Go
E56	16 Go	1520 Go
E64	16 Go	1520 Go

Tableau 10 : Configuration mémoire – processeur du Z10

IBM fournie 16 Go de mémoire supplémentaires en plus de la mémoire acheté par le client. Cette mémoire est isolée de la mémoire achetée par le client. Les données de configuration d'Entrées/Sorties sont stockées dans le Hardware System Area, appelé HSA. La mémoire supplémentaire fournie par IBM est destinée au HSA. Sur les systèmes Z10 EC, la mémoire minimum que peut commander un client est 16Go comme indiqué dans le tableau 10.

IBM System z10 EC (2097) en bref

Configuration physique	Model E12, minimum[9]	Model E64, maximum[10]
Poids	1248 kg	2271 kg
Encombrement	2,83 mètres carrés	2,83 mètres carrés
Service	5,73 mètres carrés	5,73 mètres carrés
Alimentation	9,7 kW	27,5 kW

[9] Model E12 avec une cage E/S et sans IBF (batterie interne).
[10] Model E56 avec trois cages E/S et IBF pour un total maximum de 64.

Tableau 11 : Informations sur l'IBM Z10

Le mainframe permet la vitalisation des ressources. Il est possible de partager la puissance de calcul en créant des machines virtuelles appelées : LPAR, de l'anglais « Logical Partition ». Les machines virtuelles permettent une rationalisation des ressources matérielles et contribuent à la réduction des coûts.

II.4.3.2 Architecture logicielle

Dans sa gamme de produits, IBM propose une solution logicielle complète. Ces solutions « **ouvertes** » facilitent les interactions avec les produits de différents éditeurs de logiciels.
L'architecture logicielle d'AXA se compose :

- Du système d'exploitation : z/OS
- De l'ordonnanceur : Tivoli Workload scheduler, version : 8.6
- Un générateur de scripts et de stations : E-Gen, d'International Software Company (ISC)

Afin de faciliter l'exploitation de TWS, des fournisseurs proposent des solutions pour automatiser la mise en production des stations. Ainsi, la société International Software Company propose la solution E-Gen, certifiée Iso 20000. C'est une certification des services informatiques qui garantit le respect des normes de qualité. E-Gen permet d'automatiser les processus de déploiement des scripts, des stations, des fichiers, etc. Les processus ainsi standardisés permettent l'optimisation des travaux et des flux de travaux.

II.4.4 Fiabilité et limite de fonctionnement

L'ordonnanceur permet d'exécuter plusieurs centaines ou milliers de traitements par jours. Des pics d'activités peuvent générer des ralentissements sur l'ordonnanceur à certaines heures de la journée.
L'ordonnanceur doit honorer tous les traitements programmés à la date et aux heures prévues. Certains traitements sont exécutés toutes les minutes, pouvant aller jusqu'à 720 traitements sur 12h d'activité pour un seul traitement. Ces traitements répétitifs dits « cycliques », sont susceptibles de provoquer de légers ralentissements sur l'ordonnanceur.
Des traitements sont exécutés en parallèles sur des stations trouvant sur des réseaux locaux ou étendus. En cas de perturbation sur ces réseaux, l'ordonnanceur essaiera de se reconnecter aux stations sur lesquelles les traitements doivent être exécutés. Ces traitements passeront en erreur de traitement si les stations ne sont pas accessibles.
La conception de l'ordonnanceur permet d'ajouter une priorité pour chaque station, travaux ou flux de travaux. Cette priorité permet de traiter les travaux les plus importants du point de business.
De même, il est possible de limiter le nombre de travaux dans un flux de travaux. Cette limite est comprise entre 0 et 1024 travaux par flux de travaux.

II.5 Le projet de supervision

Le projet de supervision de l'active directory a débuté en février 2012 pour s'achever en décembre 2012.
Alors que le projet s'approchait de la fin, le groupe AXA a remplacé courant 2012 son logiciel de gestion des tickets de suivi des incidents. Les deux bases sont restées actives jusqu'en novembre 2012. Tous les systèmes d'ouverture automatique de tickets de suivi d'incidents devaient basculer sur la nouvelle base avant son arrêt complet prévu début décembre 2012.

II.5.1 Le déroulement du projet

Le projet s'est déroulé en cinq phases décrites ci-dessous et sont reprises dans le planning, tableau 12.

- **L'étude du besoin**
  - Collecte d'informations
  - Etude de faisabilité
  - Les contraintes imposées par ATS

- **La recherche et le développement**
  - Recherche des outils : utilitaires
  - Développement : codage

- **Les tests et ajustements**
  - Tests de détection d'incidents
  - Tests d'ouverture automatique de tickets d'incidents
  - Ajustements : modification du code source

- **Le déploiement**
  - Mise en production sur l'ensemble des domaines

- **La formation et la livraison**
  - Formation de 2 salariés en d'ATS
  - Livraison des codes sources : pour les futurs domaines

ATS a souhaité mettre à jour son système de gestion des incidents au cours de l'année 2012. La nouvelle base n'étant pas en production, les tickets de suivi incidents ont été créés dans l'ancienne base toujours en production.
Ce changement de logiciel de gestion des incidents a nécessité une mise à jour des différents programmes sur le module d'ouverture des incidents. Le projet n'as pas subit de modification majeur liée à ce changement.

Le projet s'inscrit dans le cadre de mes activités au quotidien chez ATS. Ma connaissance de l'environnement Microsoft Windows, particulièrement l'active directory, m'a permis d'avoir les bases nécessaires pour débuter le projet.

II.5.2 Le planning et le budget

Le planning n'a pas été imposé par Olivier Manzano responsable du service. Mais il a imposé une très forte exigence en matière de communication sur la faisabilité du projet. Le projet a débuté en février 2012 et s'est achevé en décembre 2012.
La phase de recherche des outils et de développement a été la plus importante. Les programmes ont été développés en respectant les exigences d'AXA.
Le projet a été réalisé sans budget, mais pris sur le temps du travail, ce qui correspond au budget de fonctionnement. Il s'inscrit dans le cadre des initiatives locales. C'est-à-dire des projets sans budget qui contribuent à améliorer le fonctionnement du système d'information.

ID	Nom de tâche	Début	Terminer	Durée
1	Début du projet	06/02/2012	06/02/2012	0j
2	Collecte des incidents	06/02/2012	17/02/2012	10j
3	Etude de faisabilité	20/02/2012	02/03/2012	10j
4	Recherche des outils	05/03/2012	09/03/2012	5j
5	Développement des programmes	12/03/2012	29/06/2012	80j
6	Tests et ajustements	02/07/2012	20/07/2012	15j
7	Déploiement	23/07/2012	10/08/2012	15j
8	Mises à jour des programmes	24/09/2012	02/11/2012	30j
9	Tests et ajustements	05/11/2012	16/11/2012	10j
10	Re-déploiement	19/11/2012	30/11/2012	10j
11	Formation et livraison	03/12/2012	13/12/2012	9j
12	Fin du projet	14/12/2012	14/12/2012	0j

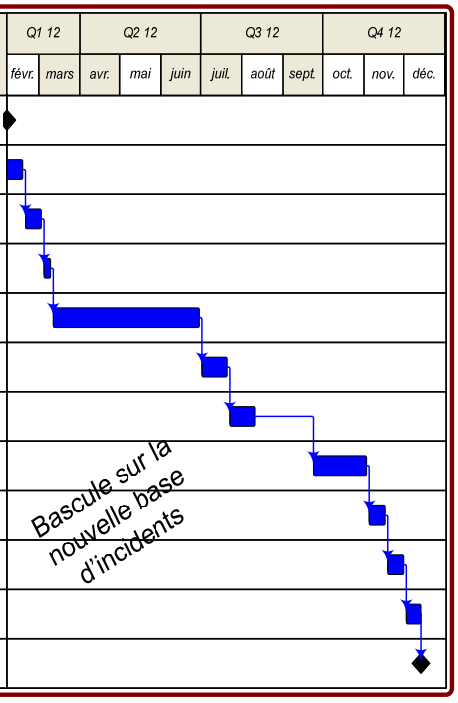


Tableau 12 : Le planning du projet

II.5.3 Les risques sur le projet

La phase d'étude de faisabilité a été décisive. La suite du projet était liée à ces résultats et à ma capacité à mener à bien ce projet de A à Z.
Les informations contenues dans les incidents collectés dans la base de gestion des incidents ont été un des éléments déterminants. De mauvaises informations ou des informations incomplètes dans les archives des tickets d'incidents m'auraient conduit sur des pistes erronées avec une perte de temps considérable.
En tant que salarié d'une société prestation informatique (SSII : Société de Services et d'ingénierie Informatique), ma mission chez ATS dépendait du contrat de service. La durée du contrat étant de 3 mois renouvelables, chacune des parties pouvait à tout moment mettre fin au contrat ou ne pas renouveler le contrat. Le projet serait alors compris.
Un autre risque non négligeable, la création automatique des tickets des incidents dans la base des incidents auraient pu compromettre la suite du projet. Car sans trace des incidents dans une base de suivie, ce projet était voué à l'échec.

II.6 En résumé

AXA Technology Services (ATS), fournisseur de services informatique, propose des systèmes d'information qui doivent répondre aux exigences du groupe AXA. La gouvernance informatique d'ATS recherche des solutions innovantes pour ses clients. Avec plus de 120000 Salarié dans le monde, le groupe AXA est une entreprise de très grande taille bien positionnée sur la scène internationale.

ATS gère une cinquantaine d'active directory, un annuaire d'entreprise basé sur les systèmes d'exploitation Microsoft Windows Serveur. Cet annuaire constitue le cœur de l'infrastructure des systèmes d'exploitation Microsoft Windows. Il permet de se connecter aux ressources de l'entreprise. Il centralise les informations nécessaires au fonctionnement de l'entreprise. Le système d'information doit être disponible sans interruption pour permettre l'accès à ces ressources. L'active directory est un des éléments indispensable à superviser.

Des incidents sur cet annuaire ont entraîné des disfonctionnements majeurs à l'échelle de l'entreprise. Les utilisateurs et de la direction du groupe ont émis des doutes sur la capacité d'ATS à proposer un système d'information stable. Les engagements de la DSI d'ATS de fournir un service de qualité n'ont pas pu être honorés.
Olivier Manzano, responsable du service en charge de l'Active directory, m'a choisi pour proposer une supervision de l'active directory.

La supervision de l'active directory ne doit pas être considérée comme de simples vérifications ou tests, mais comme la richesse de l'entreprise. Elle doit permettre aux équipes exploitantes d'être réactive et ainsi limiter les impacts sur les applications métiers et sur le fonctionnement de l'entreprise.
Afin de répondre aux exigences d'AXA, je propose une supervision faite sur mesure. Cette supervision est sans agent et sans interaction. La planification est réalisée par l'ordonnanceur TWS, déjà utilisé par AXA sur l'ensemble des serveurs.

III Mise en place de la supervision active directory

La supervision active directory permet de détecter les anomalies sur l'infrastructure et d'alerter les équipes exploitantes.
Elle permet aux équipes techniques d'être plus réactives et de réduire les disfonctionnements au sein de l'entreprise.
La supervision qui été développée permet de créer automatiquement des tickets de suivi des incidents dans la base des incidents du groupe AXA. Ces incidents sont affectés au groupe de résolution pour afin d'être tracés de sa création jusqu'à sa résolution.

III.1 Les composants de la supervision

La supervision est pilotée depuis l'ordonnanceur TWS. Elle a été conçue pour répondre aux besoins du client ATS. Elle est paramétrable depuis les fichiers de configuration.

III.1.1 Les fonctions implémentées

La supervision a été conçue afin d'alerter en cas de détection d'anomalie sur l'infrastructure active directory. Les alertes sont envoyées par courriel à une liste de diffusion se trouvant dans les fichiers de configuration. Ce courriel est aussi envoyé à une boite aux lettres pour la création d'un ticket de suivi dans la base des incidents.
L'ordonnanceur fait partie intégrante de la supervision. Il permet de planifier les cycles de contrôles.

III.1.1.1 L'automatisation de la supervision par TWS

L'ordonnanceur TWS, décrit au paragraphe II.4.3, planifie l'exécution de la supervision. La supervision est en production du lundi au samedi de 00h00 à 23h30.
Le programme principal sera exécuté toutes les 30 minutes sur chaque contrôleur superviseur. Le contrôleur superviseur est le seul contrôleur de domaine de chaque domaine sur lequel se trouvent les programmes de la supervision. La fréquence d'exécution peut être réduite et ramener à 10 minutes. Le retour d'expérience a permis d'ajuster cette fréquence au plus juste, sans trop solliciter l'ordonnanceur.
L'ordonnanceur initie un « cycle de supervision » à chaque exécution du programme centrale. Ce cycle se termine à la fin d'exécution de tous les sous-programmes. L'ordonnanceur vérifie que l'exécution des programmes s'est bien déroulée. En cas de problème sur un des programmes, un incident sera créé automatiquement dans la base de suivi des incidents groupe AXA par l'ordonnanceur lui-même.
Les administrateurs de l'ordonnanceur l'ont configuré afin qu'il créé un ticket d'incident dans l'environnement de production. La création automatique des tickets d'incidents dans la base des incidents est décrite au paragraphe IV.1.4.3.
L'ordonnanceur TWS permet d'administrer et de suivre l'état des travaux depuis une seule et même console d'administration pour l'ensemble des 50 domaines d'AXA.
La désactivation de la supervision est possible depuis l'ordonnanceur. Dans ce cas, elle affectera l'ensemble des serveurs supervisés. La fonction de « **désactivation** » a été implémentée dans la supervision, afin de limiter les taches de maintenance dans l'ordonnanceur.

III.1.1.2 Désactivation et activation de la supervision

Les analyses des incidents ont permis de mettre en évidence la nécessité d'avoir une fonction de désactivation de la supervision pour certains contrôleurs de domaine pendant les horaires de production. Lorsque les équipes d'exploitation travaillent sur la résolution de l'incident, il n'est plus nécessaire de continuer à alerter par l'envoie de nouveaux courriels.
L'activation ou la désactivation de la supervision est réalisée dans le fichier configuration « **config_ldap.ini** ». Le fichier de configuration est décrit à la section III.1.4.2
Lorsque l'incident est résolu, la supervision pourra être réactivée. La reprise de la supervision permettra de valider l'état du serveur.

- **Désactivation de la supervision**

La désactivation d'un ou plusieurs contrôleurs sera réalisée sur le serveur superviseur. Elle permet maintenir la liste des contrôleurs de domaine dans la configuration de la supervision.
La désactivation est possible en intégrant un caractère « # » en début de ligne devant le nom et l'adresse IP du contrôleur de domaine à désactiver, comme illustré ci-dessous.

- #**SERVER_NAME:**PRINTSIEGDC32
- #**IP_SERVER:**10.209.20.32

La désactivation de la supervision est recommandée si la durée de traitement de l'incident sera suffisamment longue. Elle est prise en compte dès le prochain cycle de supervision.
La désactivation de la supervision doit être exceptionnelle et non un automatisme. Elle peut être utilisée dans les cas de figure cités ci-dessous :

- Réinstallation du système d'exploitation d'un contrôleur de domaine
- Coupure électrique due aux intempéries, incendies,…
- Etc.

- **Activation de la supervision**

A la fin de la maintenance sur le contrôleur de domaine, la supervision sera réactivée par l'exploitant. La réactivation de la supervision est réalisée en supprimant le caractère inséré dans le fichier de configuration. Elle permet de vérifier que le serveur est conforme pour la remise en production.

- **SERVER_NAME:**PRINTSIEGDC32
- **IP_SERVER:**10.209.20.10

La réactivation de la supervision sur le contrôleur de domaine est prise en compte dès le prochain cycle de supervision. Il en est de même pour la prise en compte des alertes.

- **Activation et désactivation du mode maintenance**

La fonction maintenance est détaillée au paragraphe III.1.1.3. Cette option permet d'activer ou désactiver les alertes de manière automatique durant une plage horaire définie.
Le mode de maintenance sert à limiter les actions sur la configuration de la supervision durant des plages horaires destinées aux maintenances périodiques.

Il est possible de forcer l'exécution de la supervision manuellement. En exécutant le programme central ou « lanceur », un cycle complet sera réalisé sur tous les serveurs et s'arrêtera après avoir testé le dernier serveur de la liste.
La désactivation et réactivation automatique des alertes sont intégrées dans les options de la supervision. Elles sont définies dans les plages de maintenance. Ce mécanisme ne nécessite aucune intervention de la part de l'équipe d'exploitation.

III.1.1.3 La plage de maintenance

Les opérations périodiques sur l'infrastructure d'AXA sont planifiées les mardis et les jeudis à partir de 21h00. Ces opérations visent à stabiliser ou à améliorer le système d'information. La prise en compte de ces opérations périodiques est paramétrable dans les fichiers de configuration de la supervision. Aucun ticket d'incident ne sera créé durant la plage de maintenance. Une plage de maintenance globale est appliquée à l'ensemble des contrôleurs de domaines de l'active directory à superviser.
Deux options de configuration indiquent le début et la fin de la plage de maintenance.
L'infrastructure informatique s'étend sur plusieurs continents avec des fuseaux horaires différents. Les plages de maintenances ne sont pas les mêmes et prend en compte le décalage horaire avec les départements d'outre-mer (Guadeloupe, Martinique et la Réunion). La supervision prend en compte des plages de maintenance spécifiques. Cette plage de maintenance spécifique sera rattachée à chaque contrôleur de domaine qui le nécessite. Elle remplacera la plage de maintenance globale.
Dans l'exemple ci-dessous, la supervision créera les alertes à partir de 12h00 et s'arrêtera à 21h00.

- **SERVER_NAME:**PRINTSIEGDC32
- **EXECEP_TIME_STRT**:12:00:00
- **EXECEP_TIME_STP**:21:00:00
- **IP_SERVER:**10.209.10.32

Pendant la plage de maintenance, la supervision reste active, mais ne génère pas de tickets d'incident dans la base des incidents. La supervision continue à tester l'état de l'ensemble des contrôleurs et journalisent ces contrôles dans les fichiers historiques. Cette fonctionnalité permet de connaître le début de la défaillance pendant les heures de maintenance. Elle est très intéressante, pour identifier si la défaillance est liée à l'opération de maintenance. Dans l'exemple ci-dessus, elle s'étend de 21h01 à 11h59.
Le début plage de maintenance de la supervision annonce la fin de la plage de service, et inversement. La plage de service correspond aux horaires de travail pour les salariés d'AXA.

III.1.1.4 La plage de service

La plage de service représente les heures d'utilisation du système d'information par les équipes métiers, les utilisateurs, etc. Elle débute à la fin de la plage de maintenance et se termine au début de la plage de maintenance.
Des applications sont en production horaires élargies 24/24 et 7j/7j et nécessitent les services délivrés par les contrôleurs de domaine. Mais les contrôleurs de domaines ne sont pas soumis à ces contraintes horaires élargies.
Durant la plage de service, toutes les anomalies constatées et vérifiées par la supervision seront signalées par l'envoie d'un courriel aux équipes d'exploitation. Ces destinataires sont renseignés dans les fichiers de paramétrage de la supervision.
La même plage de service et les mêmes destinataires sont utilisés pour tous les domaines. Seuls les contrôleurs domaines avec un décalage horaires auront un paramétrage spécifique.
La plage de service pour les contrôleurs de domaine a été fixée : de 06h00 à 19h00.
Elle est définie de la manière suivante dans le fichier de configuration « **config_ldap.ini** » :

- **TIME_START**:06:00:00
- **TIME_END**:19:00:00

La plage de service est toujours calculée sur l'heure locale de Paris. Un calcul sera fait pour déterminer les plages de service spécifiques pour chaque région.
La plage de service permet en cas d'anomalie sur un contrôleur de domaine de créer un ticket de suivi de l'incident.

III.1.2 Création des tickets de suivi des incidents dans la base d'incidents

Le logiciel de gestion des incidents utilisé par AXA est Cornerstone de la société HP. Il permet de créer des tickets de suivi d'incidents, des demandes ou des changements. Il est utilisé par tout le groupe AXA dans le cadre de la démarche qualité.
Cornerstone intègre un connecteur de courriel, c'est-à-dire un module qui permet de récupérer les courriels reçus dans une boite aux lettres électroniques. Le connecteur permet à l'application Cornerstorne d'extraire le contenu du courriel. Si le courriel correspond au format attendu, un ticket incident sera créé automatiquement dans la base. Le format du courriel est fourni par l'éditeur HP. Il contient les mots clés correspondants à chaque champ dans le ticket de l'incident. L'incident sera affecté au groupe de résolution pour son traitement. Ce groupe est spécifié dans le courriel envoyé à l'application Cornerstorne.
Le format du courriel a été intégré à la supervision. L'équipe d'exploitation recevra en parallèle le courriel afin qu'elle soit plus réactive.
Lors de la détection d'un incident sur un ou plusieurs contrôleurs de domaine, du même domaine, un seul courriel sera envoyé par module et par cycle de supervision. Il y aura donc au maximum que cinq courriels correspondants à chacun des modules. Le courriel sera envoyé à la fin du cycle de contrôle de chaque module. La figure 18 illustre le processus simplifié de gestion des incidents par la supervision.

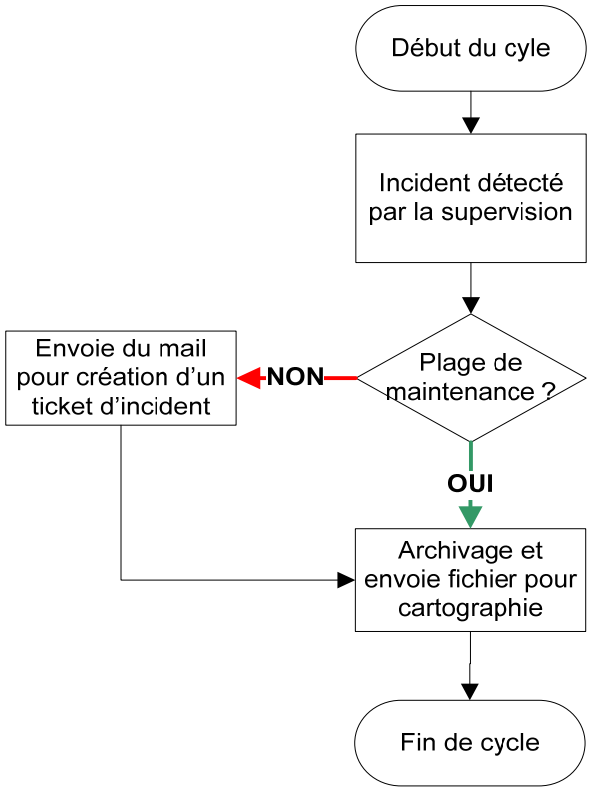


Figure 18 : Processus de gestion des incidents

Les courriels dont les formats ne sont pas conformes sont transformés en ticket d'incidents orphelins dans la base des incidents. Les incidents orphelins sont des incidents incomplets.
Le ticket de suivi des incidents sera créé avec un numéro unique dans la base des incidents. Il aura une priorité P3, comme définit au paragraphe II.2.2. La priorité pourra être réévaluée avec les gestionnaires des incidents. Le numéro d'incident permettra de le suivre et de communiquer sur son évolution si besoin.
Le suivi des incidents sur les contrôleurs de domaine est journalisé par la supervision. L'historique des événements de contrôle est sauvegardé sur le serveur superviseur.

III.1.3 L'historique des tests dans la supervision

La supervision collecte les informations sur l'ensemble des contrôleurs de domaine par le biais de tests. Ces informations sont traitées en vu de détecter des anomalies. Toutes informations collectées et traitées sont sauvegardées dans des fichiers au format texte. Les fichiers historiques permettent de rechercher des incidents survenus sur l'infrastructure AD. Les informations collectées sont horodatées pour chaque test. Elles servent à cibler le début et la fin de l'incident. Les incidents survenus sur les contrôleurs de domaines pendant la plage de maintenance ne seront pas traités dans l'application Cornerstorne. Il n'y a pas d'ouverture de ticket d'incident durant cette période. Mais les tests sont journalisés dans les fichiers des historiques pour être exploités ultérieurement.
La taille de ce fichier augmentera progressivement. Il devra être sauvegardé ou archivé une fois par an. Pour 50 serveurs à superviser sur une année, la taille d'un fichier historique sera de moins de 200Mo[26]. Il y a un fichier historique pour chaque point supervisé, soit cinq fichiers historiques au maximum par domaine.
Lorsque les fichiers historiques sont supprimés, ils seront recréés automatiquement lors de la prochaine exécution de la supervision. Si la supervision est en cours d'exécution, la suppression du fichier historique ne sera pas possible, car le fichier sera verrouillé par les différents programmes. Il faudra attendre la fin du cycle de supervision pour réaliser les opérations sur ces fichiers. La suppression de ces fichiers entraînera la perte de tout l'historique de la supervision. La sauvegarde de ces fichiers serait le plus appropriée.
L'historique des évènements permet de détecter des incidents durant les plages de maintenance. Il permet de déterminer si l'incident constaté est dû à une opération planifiée par les équipes techniques ou à est lié à un événement imprévisible.
L'historisation est un élément de traçabilité de la supervision qu'il est important de maintenir.

Ces fichiers historiques pourront servir pour réaliser des statistiques sur l'état des différents Active Directory. Le format des fichiers historiques permet un traitement automatisé des données dans un tableur du type Microsoft Excel. Les données collectées durant plusieurs mois sont importantes pour avoir une vision globale de l'état des différents contrôleurs de domaines sur toute la période. Ainsi les contrôleurs de domaines ayant rencontrés le plus d'incident pourront faire l'objet d'une attention particulière :

- Maintenance préventive
- Analyse des différentes causes : récurrentes, imprévisibles, erreur humaine ...

[26] 1Mo=1024Ko et 1Ko=1024 octets

Le tableau 13 représente les statistiques faites sur 3 contrôleurs de domaine du même domaine. Pour chaque contrôleur de domaine, il y a deux erreurs à la même heure. C'est du à une double vérification pour éviter des alertes intempestives du à des microcoupures réseaux par exemple.
Le principe de fonctionnement des tests d'authentification est détaillé au paragraphe III.2.4.

Dans l'analyse des statistiques présentées ci-dessous, les alertes ne sont pas prises en comptes. Elles sont comprises dans les plages de maintenance, présenté au paragraphe III.1.1.3.
Les contrôleurs de domaines redémarrent certains jours de la semaine à 5h00 du matin heure local.
Les deux comptes « **chk_citrix** » et « **chk_citrix2** » servent à tester l'authentification sur les contrôleurs de domaine.

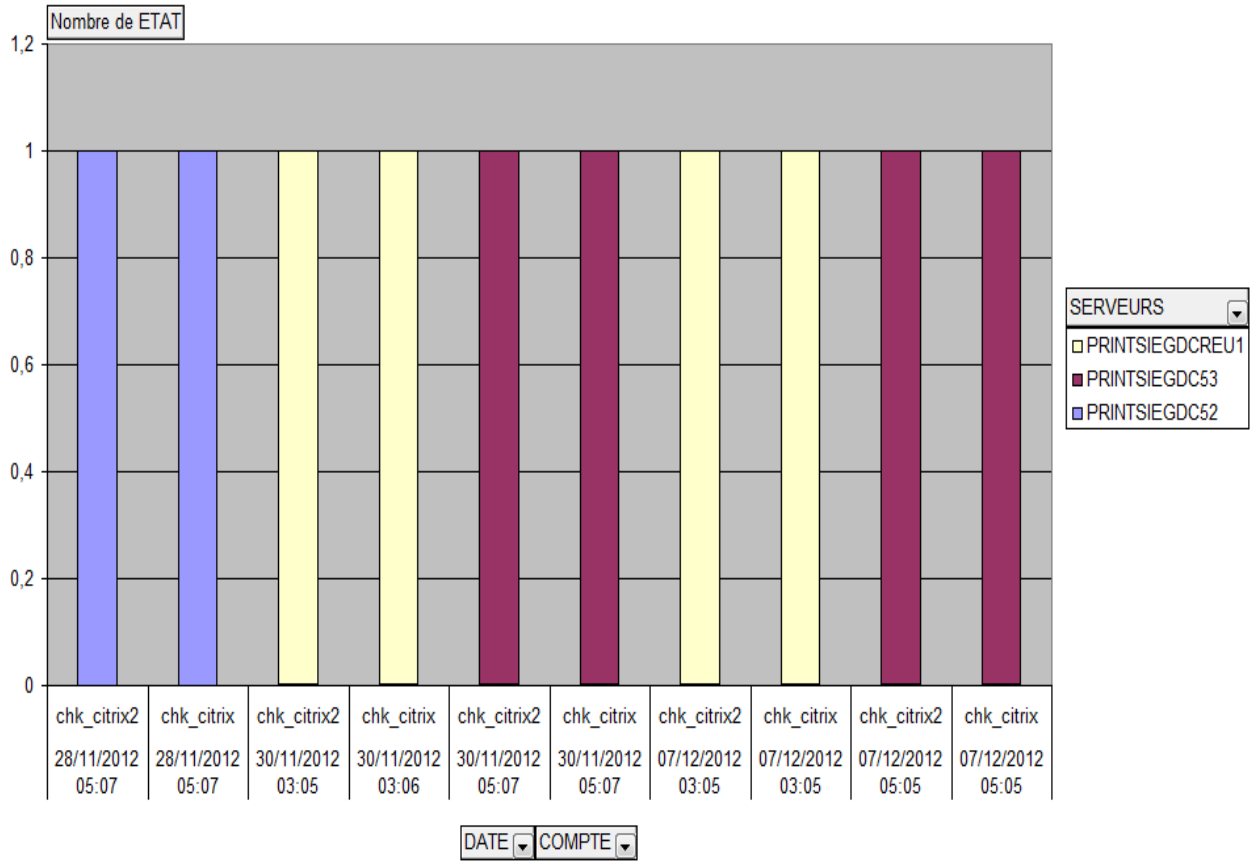


Tableau 13 : Exemple de statistique sur les incidents

L'exploitant peut à la fin de son intervention sur l'infrastructure consulter les fichiers résultats de la supervision pour s'assurer qu'il n'y a plus d'incidents en cours. Il peut aussi consulter le site intranet de la cartographie de la supervision. La cartographie fait parti d'un autre projet global de collecte et de traitement des données. Les informations collectées par de nombreux projets sont mises à disposition pour une interprétation graphique.

III.1.3.1 La cartographie des contrôleurs de domaine

La cartographie ne fait pas parti projet de supervision, mais d'un projet global de mise en forme des données collectées de différents projets. Elle sert à mettre en forme sur un site intranet des données collectées. Elle donne une vision globale de l'état de l'ensemble des domaines et des contrôleurs de domaine.
Les données collectées lors du cycle de la supervision sont copiées sur un disque réseau partagé. Un script est exécuté sur le serveur web, pour les copier dans ses répertoires de travail. Ces fichiers déjà formatés et permettent un traitement automatisé. Les champs correspondants au résultat de la supervision sont traités afin faire ressortir les anomalies sur le site intranet :

- Rouge : Critique
- Jaune : Avertissement
- Vert : fonctionnement normal

La cartographie permet d'avoir un état des contrôleurs sans avoir besoin de se connecter aux différents contrôleurs. Elle regroupe tous les domaines supervisés. Un onglet permet de séparer l'environnement de production des autres environnements : de test, développement, etc. Cette séparation permet d'avoir une vision globale de chaque environnement et de prioriser la production.
L'affichage de la cartographie n'est pas du temps réel. La mise à jour des données dépend d'une part du cycle de la supervision, et d'autre part du cycle de recopie des données sur le serveur web et de leur intégration. La mise à jour de la cartographie supprime les anciennes données du serveur web. La date et l'heure de la dernière mise à jour sont visibles au niveau du nom de chaque domaine, ce qui permet de voir les domaines dont les fichiers ne sont plus mis à jour.
Le nom de chaque fichier pour la cartographie est défini dans les fichiers de configuration.

III.1.4 Les fichiers de configuration

Les fichiers de configuration possèdent les informations sur les contrôleurs de domaine, les services à superviser, les comptes utilisateurs de tests, etc. Ces fichiers permettent de rendre générique les programmes. Les informations de personnalisation de la supervision seront dans ces fichiers. Les programmes sont développés pour être utilisés sur l'ensemble des domaines sans modification du code source.
Un modèle de fichier de configuration est fourni avec les livrables. Ce modèle doit être personnalisé pour chaque domaine. Soit environ 50 paramétrages. Certains paramètres du fichier de configuration sont communs à l'ensemble des domaines, ce qui permet de les réutiliser. Ainsi, les plages de maintenance ou les services sont presque toujours les même d'un domaine à l'autre.
Il y a deux fichiers de configuration nécessaire au bon fonctionnement de la supervision. Ces fichiers sont dans le répertoire « **config** ».

- **config_ldap.ini**
- **services.ini**

L'arborescence des dossiers est fournie avec les livrables au client. Toute modification de nom des fichiers ou tout déplacement d'un ou des deux fichiers, pourra entraîner un disfonctionnement de la supervision.
Les mots clés devront être respectés comme fournis dans le modèle. Ces mots clés permettent d'extraire les données de configuration, de délimiter une section, etc.

III.1.4.1 Le fichier de configuration services.ini

Le fichier de configuration « **services.ini** » contient la liste de tous les services à tester. Ce fichier est lu au début de chaque cycle de supervision afin de consolider les commandes à exécuter. Il contient 3 mots clés réservés, dont il faut respecter l'ordre. Les « **:** » font aussi parti du mot clé.

- **SERVICE_NAME:** contient le nom du service Windows nécessaire au fonctionnement de l'active directory et du système.
- **NO_CHECK:** indique les serveurs sur lesquels ce service ne sera pas vérifié. Cette option est importante. Si un service n'est pas présent sur un ou plusieurs contrôleurs de domaine, l'option interdit l'ouverture des incidents pour ce ou ces contrôleurs. L'utilisation de «NO_CHECK: » est facultatif.
- **SERVICE_ID:** détermine le niveau de criticité du service. L'indicateur 2 ne sera pas utilisé, car seuls les services ayant une forte criticité sur le fonctionnement de l'active directory sont pris en compte.
    - 0 = Critique
    - 1 = Warning (avertissement)
    - 2 = Faible

Le fichier de configuration contient une seule entrée pour chaque service. C'est-à-dire qu'il ne contient pas de doublon du nom de service. Mais il y aura autant des mots clés réservés « **SERVICE_NAME:** » et « **SERVICE_ID:** » que de services.

Ci-dessous deux exemples de services configurés dans le fichier «services.ini »

- Le service « **Automatic Updates** » ou « service de mise à jour automatique de Windows ». Le nom de ce service Windows est «**wuauserv**». Ce service s'il est en défaillant sera remontée par la supervision comme «Warning » ou avertissement. Car l'active directory pourra toujours fonctionner, mais les mises à jours de sécurités ne pourront pas être pas installées.

  # Automatic Updates
  SERVICE_NAME: wuauserv
  SERVICE_ID:1

- Le service «**PassGo Access Control Agent**» dont le nom Windows est « **MyPriAgent** » sert à l'authentification centralisée des utilisateurs. Ce service permet aux utilisateurs de se connecter à des applications se trouvant dans différents domaines avec un seul et unique mot de passe. C'est l'outil de gestion du « single sign on », appelé « SSO ». Le SSO est l'authentification unique dans l'environnement multi-domaines.

  #PassGo Access Control Agent
  SERVICE_NAME: MyPriAgent
  NO_CHECK:PRINTSIEGDCX1;PRINTSIEGDCX2;PRINTSIEGDCX3
  SERVICE_ID:0

Tous les services Windows ne seront pas ajoutés dans le fichier de configuration. Les services nécessaire au bon fonctionnement de l'active directory y figureront. Le fichier indispensable et incontournable est le fichier « **confi_ldap.ini** ». Il contient entre autre la liste des serveurs à superviser.

III.1.4.2 Le fichier de configuration config_ldap.ini

Le fichier de configuration «**config_ldap.ini**» est la valeur ajoutée de la supervision. Il se trouve dans les livrables, dans le répertoire « **config** ». Il est lu au début de chaque cycle de supervision pour en extraire les informations. Ce fichier renferme toute la technologie déportée de la supervision. Il transforme la supervision en supervision générique, utilisable dans tous les environnements active directory. Il contient les mots clés réservés qu'il convient de respecter pour le bon fonctionnement de la supervision. Il est unique dans chaque domaine. Un extrait du fichier de configuration est fourni ci-dessous :

- Les informations d'identification du domaine
  - **DOMAINE:** Contient le préfixe des fichiers de logs pour la cartographie
  - **CHK_DOMAINE:** Le nom du domaine Active Directory
    - **Ex : DOMAINE:**AFA.SIEGE_DCC
    - **CHK_DOMAINE:**SIEGE

- Les informations des comptes de test
  - **USER:** Compte à tester, ce compte doit exister dans l'active diectory
  - **PASS_WORD:** identificateur numérique unique qui contient le mot de passe du compte **USER:**
    - **USER:**chk_citrix
    - **PASS_WORD:**0

    Le mot de passe du compte chk_citrix correspond à l'indice 0. L'indice 0 a une correspondance avec le vrai mot de passe dans les programmes

- Les plages de maintenance et de service
  - **TIME_START:** Heure de début de prise en compte des alertes pour la création des tickets d'incidents
  - **TIME_END:** Heure de fin de création des incidents
    - **TIME_START:**06:00:00
    - **TIME_END:**19:00:00

Le fichier de configuration contient d'autres informations :

- Type de domaine : Enfant (C : Child) ou Parent (R : Root)
- L'adresse mail pour la création des tickets d'incidents
- Le groupe d'affectation des incidents dans la base de gestion des incidents
- Les destinataires qui recevront en copie le courriel (équipe exploitante)
- L'adresse IP du serveur de messagerie ou relais de messagerie.
- Etc.

Au début de chaque cycle les informations contenues dans le fichier sont extraites afin de créer les commandes qui seront ensuite exécutées. Ces commandes sont crées de manière dynamiques.

Note :

- Les fichiers de configuration et les répertoires fournis ne doivent pas :
  - être renommés.
  - être déplacés.

Le fichier de configuration «**config_ldap.ini**» est fourni en annexe 4.

III.2 Fonctionnement de la supervision

La supervision sert à l'automatisation des tests sur l'ensemble des contrôleurs de domaine. L'ordonnanceur TWS planifie l'exécution du programme principale sur chaque contrôleur superviseur. Le programme principal est appelé « LANCEUR », il est illustré sur la figure 19.

III.2.1 Le lanceur

Le lanceur est le programme principal de la supervision. Il est chargé d'exécuter l'ensemble des sous programmes dans un ordre défini. Lors de l'exécution d'un sous programme, le lanceur s'assure que celui-ci est bien terminé avant de lancer le suivant. Le lanceur ne vérifie pas les plages de maintenance ou de service. Le lanceur est identifié par le script appelé « **GO_IVP.VBS** ».
Il est développé en Visual Basic Script. Sa fonction principale est d'être l'interface entre l'ordonnanceur TWS et les sous-programmes. Il libère le traitement de l'ordonnanceur TWS lorsque tous les programmes du cycle de la supervision sont terminés.

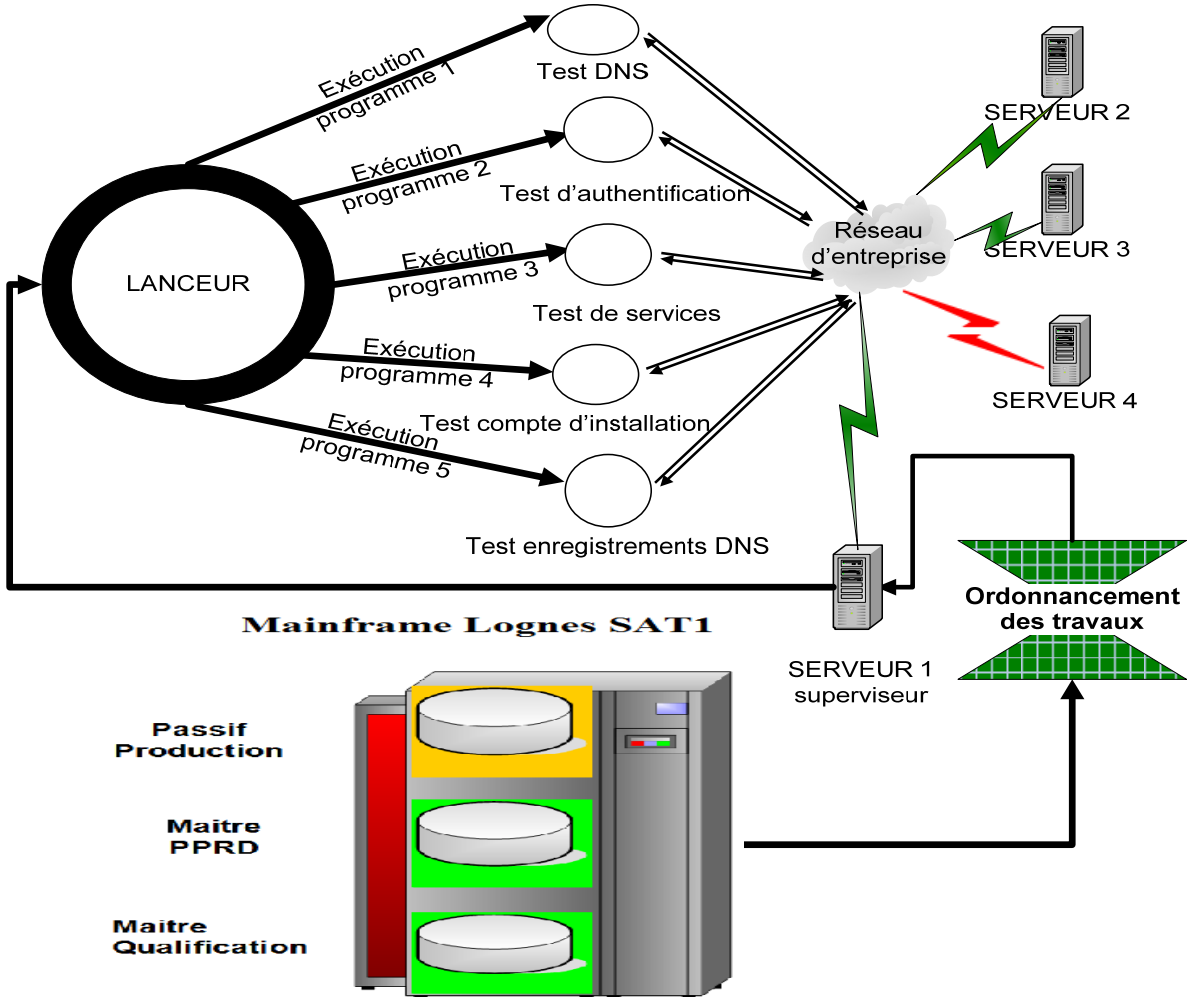


Figure 19 : Le principe de la supervision d'active directory

Lorsqu'une anomalie est détectée sur le lanceur ou les sous programmes, un ticket d'incident sera ouvert par l'ordonnanceur dans la base des incidents d'AXA, Cornerstorne. Le serveur superviseur sera alors vérifié pour déterminer l'origine de ce disfonctionnement.

Les fonctions du lanceur sont basiques, mais elles permettent de réduire le nombre de traitement dans l'ordonnanceur TWS. Un seul traitement pour cinq fonctions dans la supervision. La supervision des services Windows est possible grâce au lanceur. Les services Windows sont testés pour vérifier leur état.

III.2.2 La supervision des services Microsoft Windows

Certains services de Microsoft Windows sont indispensables pour le bon fonctionnement de l'Active Directory. La liste des services et des serveurs à superviser sont renseignées dans les fichiers de configuration. Une requête est lancée depuis le serveur superviseur vers le serveur supervisé. La requête est une commande native de Microsoft Windows. La commande « **SC** » pour « **Service Control** », ou contrôle de service en français, permet de gérer les servies, localement ou à distance. Une aide est disponible sur Windows en tapant la commande « **SC** » dans une invite de commande. La commande permet de connaître toutes les propriétés du service. Il est ainsi possible de connaître le statut du service : Arrêté, démarré, en cours de démarrage, etc. La supervision vérifiera que le service est en statut : « DEMARRE ».
Lorsqu'un service n'est pas en statut « DEMARRE », la supervision stocke le nom du serveur et du service dans un tableau temporaire. A la fin du cycle de supervision des services, la supervision testera à nouveau tous les services non démarrés. Si à l'issue de ce second test le service n'est toujours pas démarré, ces services seront positionnés au niveau de la supervision comme étant en « incident ».
Lorsqu'un serveur n'est pas disponible, le mécanisme est le même. Tous les services à superviser sur le serveur seront positionnés dans le tableau temporaire. Ces services seront vérifiés une seconde fois en fin de cycle. Lorsqu'un serveur n'est pas accessible depuis le serveur superviseur, il génère de la latence, c'est-à-dire, du temps d'attente pour chaque réponse de requête. Cette latence est du au fait que la requête attend pendant un délai défini par la commande avant d'abandonner. Ce phénomène est plus connu sous le nom anglais de « Timeout ». Une optimisation de la supervision sera faite ultérieurement par les équipes d'ATS en charge de l'Active Directory.
La supervision des services est nécessaire. Les services Windows sont l'une des causes principales d'incidents.
Dans la configuration de la supervision, chaque service aura une criticité qui lui est affectée. Elle permettra d'être exploitée pour la cartographie, voir paragraphe III.1.3.1. Cette criticité permet de savoir si ce service a une incidence importante sur le fonctionnement de l'active directory. Elle est sous forme numérique allant de 0 à 2 dans le fichier de configuration.

- 0 = Critique
- 1 = Warning (avertissement)
- 2 = Faible

Seuls les indicateurs 0 et 1 sont utilisés, même si la supervision intègre l'indicateur numérique 2. Lorsqu'un service est arrêté avec un indicateur 0, il apparaîtra dans les fichiers historiques ou de production sous la mention « CRITIQUE ». La liste des services et leur criticité ont été déterminées lors de la phase d'étude et de faisabilité du projet. Il est donc important de connaître les services et leur conséquence sur l'active directory. Cette remarque est à prendre en compte dans le cadre de nouvelles versions de Microsoft Windows Serveur.
Le service DNS, ou système de nom de domaine en français, est le service qui est charger de résoudre les noms de domaine en adresse IP et inversement.

III.2.3 La résolution de noms : DNS

La supervision DNS consiste à vérifier que les serveurs DNS installés sur l'ensemble des contrôleurs de domaine sont en mesure de répondre aux différentes requêtes de résolution de noms. Les applications dans l'entreprise sont de plus en plus nombreuses, souvent accessibles depuis un navigateur internet. Les applications hébergées à l'extérieur de l'entreprise nécessitent une résolution du nom de domaine. C'est le cas pour accéder au moteur de recherche : « www.google.fr ».

III.2.3.1 La résolution DNS

Chez ATS, tous les contrôleurs de domaine ont le rôle de serveur DNS intégré à l'active directory. Le serveur DNS, permet de résoudre les noms de domaines de tous les domaines accessibles sur Internet, mais aussi certains domaines internes.

- **Principe de fonctionnement d'un DNS**

Un utilisateur souhaite accéder à google.fr depuis son navigateur Internet, identifié par le point **1** sur la figure 20. Une requête est envoyée au serveur DNS afin de résoudre le nom DNS : **google.fr**. Cette requête consiste à connaître le ou les adresses IP associées à **google.fr**. Le serveur DNS s'il possède les informations demandées, figure 20 point **2**, les renvoie au client. Le client récupère ainsi l'adresse IP associée à sa demande, et se connecte à « google.fr » par son adresse IP. Le cas de « **google.fr** » est particulier, car il utilise la fonction « **round robin** » du DNS, ou tourniquet en français. Cette fonctionnalité permet la redondance des serveurs à contacter.

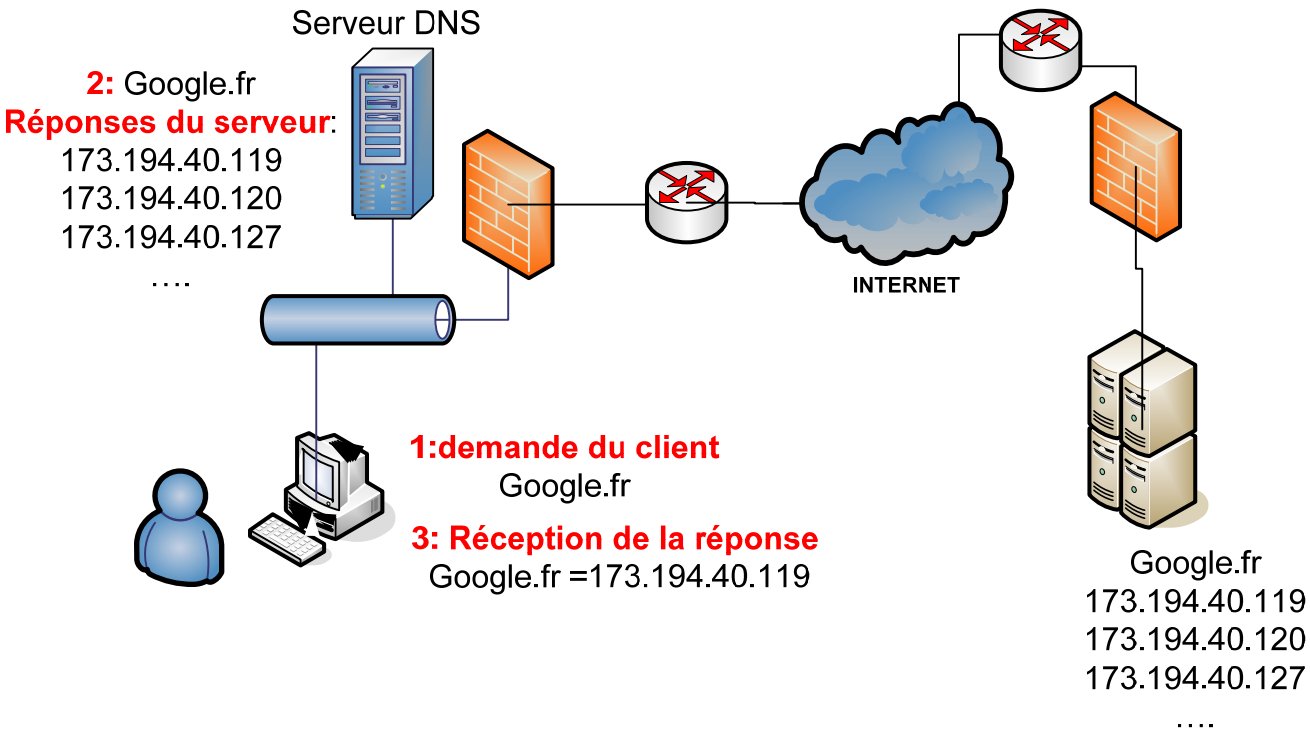


Figure 20 : Principe de fonctionnement résolution DNS

Les contrôleurs de domaine du domaine « **axa-fr.intraxa** », sont en mesure de répondre à des requêtes relatives à ce même nom de domaine. Le test de supervision consistera donc à tester si un contrôleur de domaine est en mesure de s'auto-interroger. Si le serveur répond à la requête de résolution de noms sur son propre domaine, le test est validé.
Lorsque le serveur DNS du contrôleur de domaine n'est pas en mesure de répondre à la requête, la supervision interprète le résultat des commandes, afin de générer un ticket d'incident. Ce ticket d'incident est créé selon le principe décrit au paragraphe IV.1.4.3. Les informations permettant d'identifier le serveur impacté sont renseignées dans le ticket d'incident. Elles fournissent les éléments nécessaires pour identifier le problème.
La résolution de nom DNS permet aussi à des applications d'accéder à d'autres applications de l'entreprise. L'ordonnanceur est un exemple concret. Il interroge les serveurs DNS afin de se connecter et exécuter les traitements sur les stations. Si les serveurs DNS interrogés ne répondent pas à ses requêtes, les traitements ne seront pas exécutés. Les conséquences peuvent être alors très importantes pour ATS et ses clients.
La résolution de noms DNS est un enjeu majeur pour les applications intranet ou internet. La supervision de la résolution de noms DNS permet d'alerter les équipes exploitantes afin de d'être réactif. L'analyse des incidents à montré que le service DNS pouvait être démarré et vu comme opérationnel, alors qu'il n'y avait pas de la résolution de noms sur ce contrôleur de domaine.
La commande « ***NSLOOKUP*** » est utilisée pour les tests sur le DNS. Elle est native à toutes les versions de Microsoft Windows. C'est à dire, présente sur l'ensemble des systèmes d'exploitation fournis par Microsoft. L'aide de la commande est disponible en tapant dans une invite de commande : « **nslookup / ?** ».

Utilisation :

```
nslookup [-opt ...]            # mode interactif utilisant le serveur par défaut
nslookup [-opt ...] - serveur   # mode interactif utilisant 'serveur'
nslookup [-opt ...] hôte        # recherche 'hôte' en utilisant le serveur par défaut
nslookup [-opt ...] hôte serveur        # recherche 'hôte' en utilisant 'serveur'
```

Cette aide est très peu détaillée, mais permet néanmoins d'exécuter les commandes adéquates. Cette commande ne permet pas l'export de la base DNS pour des traitements en masse. L'utilitaire « **DNSCMD.EXE** », présent dans les outils d'administration système Microsoft Windows, permet de plus de souplesse.

III.2.3.2 La résolution ciblée des enregistrements DNS

L'accès aux ressources de la société nécessite de résoudre les noms de serveurs en adresse IP. Des enregistrements critiques sont supervisés afin de s'assurer que ceux-ci sont toujours présents ou n'ont pas changé ou été supprimé. Dans des grandes entreprises comme AXA, des milliers d'utilisateurs accèdent à la même ressource grâce à la résolution de nom du DNS.
La supervision exportera la base DNS dans un fichier texte. Les enregistrements contenus dans le fichier exporté sont comparés avec les informations contenues dans les fichiers de configurations. Si les informations ne sont pas cohérentes, elles seront traduites en ticket d'incident.
La commande suivante permet d'exporter toute la zone dans le fichier « **dns_zone.txt** ».

- **dnscmd.exe IP_serveur_dns /ZonePrint nom_zone_dns > dns_zone.txt**
- **dnscmd.exe 10.210.200.20 /ZonePrint axa-fr.intraxa > dns_zone.txt**

Quelques options de l'utilitaire « **DNSCMD.EXE** » sont fournies en annexe 2.
Lorsqu'un enregistrement DNS critique est supprimé du DNS ou est modifié, un ticket d'incident sera créé dans la base des incidents. Les informations nécessaires pour identifier l'anomalie seront détaillées pour aider à la résolution de l'incident. Si l'adresse IP d'un enregistrement critique est modifiée dans le cadre d'un changement, elle devra être reportée dans les fichiers de configuration du serveur superviseur concerné.
La liste des enregistrements a été fournie par le responsable du service IDST Windows en accord avec les responsables métiers.
Ces informations sont présentes dans le fichier « **config_ldap.ini** ». Elles sont identifiées par des mots clés selon 2 cas de figures :

- **CAS 1** :
  - **NS_CONTROLE_N:** Nom du serveur
  - **NS_CONTROLE_I:** IP du serveur
- **CAS 2** :
  - **NS_CONTROLE_N**: Nom du serveur
  - **NS_CONTROLE_I:** IP du serveur
  - **NS_CONTROLE_A:** Alias du serveur

Un alias DNS est un enregistrement de type « CNAME[27] ». Il se prononce « cénèïme ». Il permet d'accéder à un serveur en utilisant un nom différent, comme illustré ci-dessous.

enregistrement	Type	Cible
PRATSSRV01	A	10.232.10.21
portail.axa.fr	CNAME	PRATSSRV01
agences.axa.fr	CNAME	PRATSSRV01

Tableau 14 : Exemple d'alias (CNAME)

Dans le fichier de configuration « **config_ldap.ini** », chaque enregistrement critique sera défini selon le **CAS 1** ou le **CAS 2**. Les enregistrements qui ne répondront pas à ces critères dans le fichier de configuration ne seront pas pris en compte.
Une des fonctions premières de l'active directory est l'authentification des comptes utilisateurs. Elle permet d'accéder aux ressources de l'entreprise.

[27] CNAME : Canonical Name, nom canonique en français

III.2.4 L'authentification des comptes

L'authentification des comptes est une fonction essentielle de l'active directory. Elle permet aux utilisateurs de se connecter aux différentes ressources de l'entreprise. Durant les évolutions de Microsoft Windows Serveur, la sécurité a été renforcée et le système a gagné en stabilité, mais des défaillances du système sont toujours possibles.
La supervision permet de surveiller que les utilisateurs peuvent se connecter en saisissant leur identifiant et mot de passe. Deux comptes utilisateurs de tests ont été créés afin de valider que les contrôleurs de domaine sont opérationnels. Les deux comptes sont testés individuellement sur chaque contrôleur de domaine. Si sur un contrôleur de domaine un seul des comptes valide le couple identifiant/mot de passe, la supervision validera l'authentification pour ce contrôleur de domaine. Si aucun des deux comptes n'a pu s'authentifier sur ce contrôleur de domaine, la supervision mettra ce contrôleur de domaine dans un tableau temporaire.
A la fin de la vérification des comptes sur l'ensemble des contrôleurs de domaine, la supervision testera de nouveau l'ensemble les deux comptes sur les contrôleurs de domaine se trouvant dans le tableau temporaire. A l'issue de ce second test, si l'authentification est validée pour au moins sur l'un des comptes, la supervision validera le bon fonctionnement de ce domaine contrôleur. Dans le cas contraire, un seul ticket d'incident sera créé pour l'ensemble des contrôleurs de domaine se trouvant dans le tableau temporaire et n'ayant pas validé au moins un des deux comptes lors du second test.
La figure 21 illustre le principe du test réalisé. Lors du premier passage du « **test 1** », le DC5 n'authentifie aucun des deux comptes. C'est aussi le cas lors du second passage du « **test 2** ». Dans ce cas, le DC5 est considéré comme défaillant pour le test d'authentification.

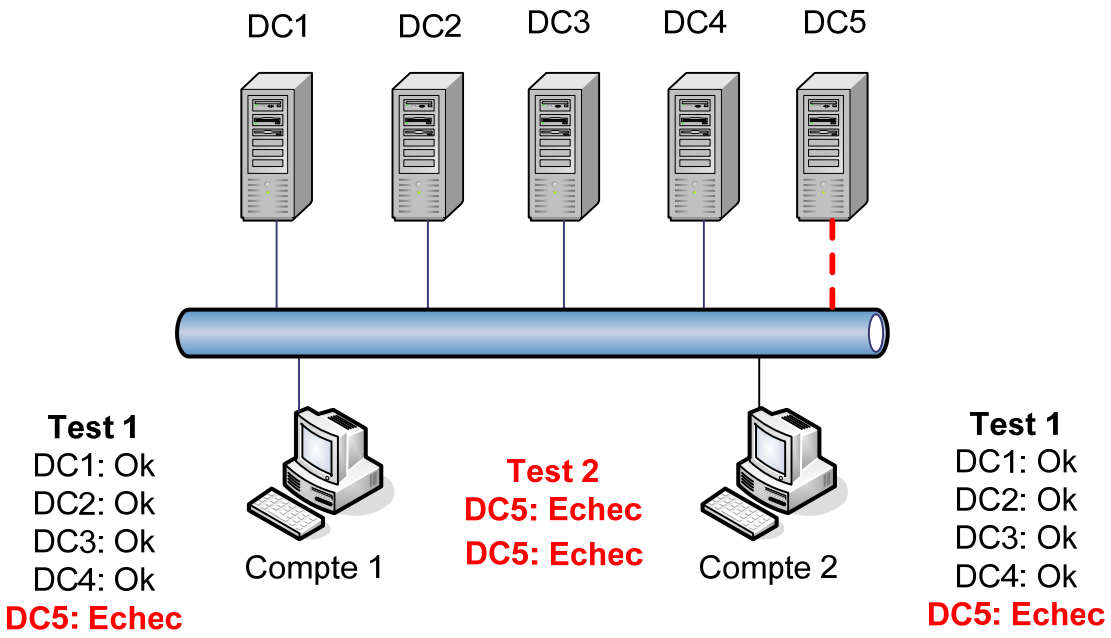


Figure 21 : Simulation authentification compte utilisateur

Le principe de l'ouverture de l'incident est présenté au paragraphe IV.1.4.3. Un courriel est envoyé à la boite aux lettres de l'application Cornorstorne du groupe AXA. Le courriel contient l'ensemble des informations nécessaire pour identifier le contrôleur ou les contrôleurs de domaine défaillant(s). L'authentification des comptes ne concerne pas que les comptes utilisateurs. Il permet aussi de valider les comptes des ordinateurs dans le domaine. Des opérations non visibles par les utilisateurs sont réalisées par les ordinateurs du domaine.

Au démarrage d'un ordinateur, il cherchera à s'authentifier dans le domaine auquel il appartient et à son site de rattachement, voir paragraphe II.3.1.1. Ce mécanisme fonctionne de la même manière que pour les comptes utilisateurs. Le test d'authentification des comptes sur un contrôleur de domaine permet de s'assurer que ce mécanisme est opérationnel.
L'authentification permet à un compte déjà authentifié sur un contrôleur de domaine d'accéder à des ressources de l'entreprise. Si la ressource nécessite une authentification, celle-ci devra être de nouveau validée. Le fait de s'être authentifié une fois, ne garantit pas l'accès à toutes les ressources, même si le compte de l'utilisateur a les autorisations d'accès suffisantes. Les contrôleurs de domaine servent à valider l'accès à toutes les ressources nécessitant une authentification Windows.
Certaines applications nécessitent un compte utilisateur, appeler le plus souvent compte de service. L'installation des serveurs chez AXA nécessite un compte d'installation pour la finalisation du serveur. Ce compte sert à l'industrialisation des installations des serveurs.

III.2.5 Les comptes d'industrialisation de serveurs

Le compte d'industrialisation ou d'installation est compte qui permet la finalisation de l'installation des serveurs. Il sert à l'intégration du serveur dans le domaine de manière automatique. Dans le cadre de la « **VM[28] on Demand** » chez AXA, machine virtuelle à la demande en français, les flux de travaux qui permettent de délivrer des serveurs en moins 4 heures utilisent aussi le compte d'installation. Cette chaîne d'industrialisation est importante pour ATS, car c'est un nouveau service proposé à ses clients.
La supervision de ce compte d'installation permet de s'assurer que les installations ne seront pas bloquées, si le compte est verrouillé par exemple.
Ce test est basé sur le même principe que l'authentification des comptes, décrit au paragraphe III.2.4. La seule différence, c'est qu'il n'y a qu'un seul compte d'installation par domaine.
Le compte sera testé sur chaque contrôleur de domaine. Si l'authentification est validée, la supervision passera au contrôleur de domaine suivant, et ainsi de suite. Si l'authentification est en échec, le contrôleur de domaine sera mis dans un tableau temporaire. En fin de vérification sur l'ensemble des contrôleurs de domaine, les contrôleurs de domaine présents dans le tableau temporaire seront de nouveau testés. Si le test est en échec, l'authentification sera alors considérée comme défaillante. A la fin des tests sur avec le compte d'installation sur tous les contrôleurs de domaine présents dans le tableau temporaire, un seul incident sera créé en cas d'échec d'authentification. Cet incident contiendra le nom du contrôleur, le domaine et le nom du compte en échec.
Si le compte d'installation est verrouillé sur contrôleur de domaine, le principe de l'active directory est de répliquer tous les changement entre les différents contrôleur de domaine. Ce compte sera lors verrouillé sur l'ensemble des contrôleurs de domaine du même domaine. Ce compte d'installation sert aussi pour les installations de serveurs manuelles. Une erreur humaine peut être à l'origine de ce verrouillage après plusieurs tentatives infructueuses. La supervision détectera une erreur d'authentification. Car lorsqu'un compte est verrouillé, il n'est pas possible de s'authentifier avec ce compte.
L'intervention des équipes techniques sera alors nécessaire pour revenir à un fonctionnement normal. En déverrouillant le compte sur un contrôleur de domaine, le déverrouillage se propagera sur l'ensemble des contrôleurs du même domaine. Ainsi il évite d'intervenir sur l'ensemble des contrôleurs.

[28] VM = Virtual Machine en anglais, ou Machine Virtuelle en français

III.3 L'architecture de la supervision

L'architecture de la supervision permet d'avoir les éléments indispensables pour sa conception. Les utilitaires et langages de programmation seront abordés. Le serveur principal de la supervision est appelé « **serveur superviseur** ».

III.3.1 Les langages de programmation

Afin de respecter les exigences d'AXA en matière de sécurité, les outils utilisés sont natifs au système d'exploitation ou disponible gratuitement sur le site de Microsoft. Aucun autre programme ne sera utilisé dans le cadre du projet de la supervision.

III.3.1.1 Les commandes DOS

Le DOS[29] ou MS-DOS[30] a été créé par la compagnie Microsoft en 1981. Le DOS était alors un système d'exploitation à part entière destiné aux ordinateurs de la compagnie IBM[31]. Les ordinateurs d'aujourd'hui utilisent leur propre système d'exploitation comme Microsoft Windows. Le DOS a évolué et est aujourd'hui sous forme d'interpréteur de commandes.
Les commandes DOS sont très utilisées car elles permettent des opérations en mode texte. Le système d'exploitation Microsoft Windows accepte deux modes de connexions :

- Le mode intégratif : un utilisateur ouvre une session et se connecte au bureau Windows
- Le mode non-interactif : Une tache est exécutée avec le compte de l'utilisateur en tache de fond sans que celui-ci n'ait accès au bureau de Windows

L'exécution de logiciels en mode non-interactif s'avère assez fastidieux, surtout s'il doit interagir avec l'utilisateur. Les commandes DOS permettent une exécution en mode « **tache de fond** ». L'interaction se fait via les options passées en paramètres. Tous les logiciels ne sont pas conçus pour un mode non-interactif.
La supervision utilise l'interpréteur de commandes DOS pour fonctionner en tache de fond. Les interfaces utilisateurs ou Interface Homme-Machine (**IHM**) ont été inhibées et remplacées par des contrôles continus.
Les « **batches** » sont des fichiers non compilés (fichier texte) qui permettent d'enchaîner plusieurs commandes à exécuter.

III.3.1.2 Le batch

Le batch est un enchaînement de commandes. Il est utilisé pour l'automatisation de traitements. Il n'est pas un langage de programmation, mais un fichier contenant les instructions à exécuter. Ces instructions peuvent être des commandes DOS, des exécutables, des scripts, des utilitaires, etc. Ces instructions sont sous la forme de lignes de commandes.
Sur les systèmes d'exploitation Microsoft Windows, les deux fichiers batches les plus utilisées ont les extensions :

- **.BAT**
- **.CMD**

[29] DOS : Disk Operating System
[30] MS-DOS : Miscosoft Disk Opérating System
[31] IBM : International Business Machine

Ce sont des fichiers « textes» non compilés, consultables ou modifiables depuis n'importe quel éditeur de texte.
L'un des avantages du batch est de pouvoir créer des scénarios. Ces scénarios sont possibles en récupérant les codes retour d'exécution des commandes. Les codes retour décrivent l'état du traitement ou du système. Les scénarios sont très utilisés comme solution de contournement.
La supervision intègre un générateur de batches. C'est-à-dire que les batches sont créés à la volée. Il est possible que ces bacthes ne soient pas identiques d'une exécution à l'autre, car ils sont dynamiques. Ce générateur lit les fichiers de configuration, pour créer les commandes à intégrer dans les différents batches.
Ils peuvent faire appel à d'autres batches ou des scripts écrits dans d'autres langages de programmation. Le principal langage de programmation utilisé pour créer la supervision est le Visual Basic Script.

III.3.1.3 Le Visual Basic Script (VBS)

Le Visual Basic Script (**VBS**) est un langage de programmation très utilisé par les administrateurs ou ingénieurs système Windows. Il permet d'automatiser les contrôles, de réaliser des opérations sur le système Microsoft Windows. Le compilateur Visual Basic est natif à toutes versions de Windows. Ce compilateur est en réalité un interpréteur de ligne de commandes. Le Visual Basic Script permet d'exécuter des programmes au format « **.vbs** ». Ces fichiers sont éditables avec n'importe quel éditeur de texte. Comme tous les langages de programmation, le VBS comporte des mots réservés. Ce sont des mots clés qui ne peuvent être utilisés que pour le codage et non pour identifier une variable. La portée des variables est une notion importante, c'est ce qui détermine si la variable sera utilisée dans l'ensemble du programme ou limitée à une seule fonction ou « section ».
Les programmes de la supervision sont développés en VBS, ce qui permet une évolution du code sources par les administrateurs ou ingénieurs système. Les fonctions intégrées au VBS permettent de faire appel à des programmes extérieurs, comme les programmes intégrés à Microsoft Windows. Ces fonctions peuvent aussi d'exécuter des scripts, des commandes Windows ou des commandes DOS.
Les commandes natives à Windows sont intégrées dans les programmes développés en VBS. Cette intégration des commandes est souvent appelée « encapsulation ». La supervision utilise la génération de scripts, c'est-à-dire, qu'à partir d'une ou plusieurs lignes de commandes de générer un fichier exécutable. Cela permet de rendre le programme dynamique en régénérant à chaque fois ces fichiers exécutables.
La supervision utilise des utilitaires Windows, des programmes sans interface graphique.

III.3.2 Les utilitaires Windows

Les utilitaires Windows utilisés dans le cadre de la supervision sont des programmes intégrés de bases à Windows ou développés par Microsoft. Aucun autre utilitaire n'a été utilisé afin de respecter le cahier des charges. Tous les utilitaires utilisés sont exécutables en lignes de commandes, sans interface graphique. Ce mode permet une exécution en arrière plan ou tache de fond.

- **La supervision des enregistrements DNS utilise l'utilitaire : DNSCMD**
  - **DNSCMD**: interface de gestion du DNS en ligne de commande. Cet utilitaire téléchargeable depuis le site de Microsoft permet de gérer en ligne de commande le service DNS. Il permet d'afficher ou d'exporter le contenu de la base DNS. Les options sont disponibles en annexe 2.

- **La supervision des services**
  - **SC**: est un utilitaire de ligne de commande utilisé pour communiquer avec le Gestionnaire de contrôle des services et les services. Les options de la commande sont disponibles en annexe 3.

- **La supervision de nom DNS**
  - **NSLOOKUP**: est un utilitaire commun à toutes les versions de Windows. Il sert à interroger un serveur DNS. Les commandes sont fournies au paragraphe III.2.3.1

Tous les utilitaires nécessaires au bon fonctionnement de la supervision seront fournis dans les livrables. Ces utilitaires ne nécessitent pas d'installation, c'est-à-dire qu'ils sont utilisables directement en les copiant sur le serveur superviseur.

III.3.3 Le serveur superviseur

Le serveur superviseur est un contrôleur de domaine qui a accès à l'ensemble des contrôleurs de domaine du même domaine. C'est-à-dire, que les éventuels pare-feux présents entre les différents contrôleurs de domaine, autorisent la communication avec le serveur superviseur. Afin d'optimiser la supervision et réduire les temps de réponses, ce serveur superviseur sera sur le site central. Ce site offre de meilleurs temps de réponses vers l'ensemble des autres sites : Province, DOM, etc. Il n'y a qu'un seul serveur superviseur par domaine active directory. Il est le cœur de l'architecture de la supervision. Il possède l'ensemble des scripts et utilitaires nécessaires pour le fonctionnement de la supervision. Aucun programme ne sera copié ou nécessaire sur les autres contrôleurs de domaine.
La fonction principale du serveur superviseur est d'exécuter les travaux programmés par l'ordonnanceur TWS. Le serveur superviseur remplit les deux fonctions ci-dessous :

- **La fonction de serveur superviseur**
- **La fonction de serveur supervisé**

Il supervise l'ensemble des serveurs du même domaine et lui-même par la même occasion. Lorsque le serveur superviseur est en maintenance, la supervision peut être compromise. Il convient alors de déplacer placer la supervision sur un autre serveur si la maintenance venait à se prolonger.
Le rôle de superviseur peut être transféré sur un autre contrôleur de domaine. Dans ce cas, il faut s'assurer de respecter les exigences ci-dessous :

- Le traitement de l'ordonnanceur TWS est modifié pour exécuter les travaux sur le nouveau serveur superviseur.
- Les livrables contenants les scripts sont copiés sur le nouveau serveur superviseur
- Le nouveau serveur superviseur accède à l'ensemble des autres contrôleurs de domaine

Les programmes ont été conçus afin que tout transfert de rôle de superviseur soit transparent lorsque les points ci-dessus ont été respectés. Il n'y a aucune installation de logiciels pour réaliser la supervision, ce qui facilite la mise en place du serveur superviseur.
Le serveur superviseur est le point central de la supervision de l'active directory. Des améliorations sur la supervision sont possibles, notamment en matière de performance.

III.4 Evolutions et performances

La supervision a été développée dans un langage permettant son évolution vers d'autre langage de programmation. Les tests de performances réalisés sont acceptables pour une infrastructure active directory de cette taille.

III.4.1 Evolution vers une supervision redondante

La supervision a été conçue afin de répondre aux exigences d'ATS. L'ordonnanceur TWS permet de créer des scénarios, comme indiqué dans la figure 22. L'utilisation des scénarios permettrait de créer une supervision redondante.

- **Scénario envisageable**
  - Serveur superviseur principale : **Contrôleur 1**
  - Serveur superviseur secondaire : **Contrôleur 2**
    - Les programmes de la supervision seraient copiés sur les deux serveurs

La supervision principale serait exécutée sur le **contrôleur 1**. En cas d'anomalie d'exécution du programme de la supervision sur ce serveur, il serait exécuté sur le **contrôleur 2**, serveur secondaire de la supervision. Ce scénario est illustré dans la figure ci-dessous.
Les **travaux N2** en échec sur le **contrôleur 1** seraient transférés sur le **contrôleur 2**. Les travaux suivants seraient exécutés sur le contrôleur principal (**contrôleur 1**).

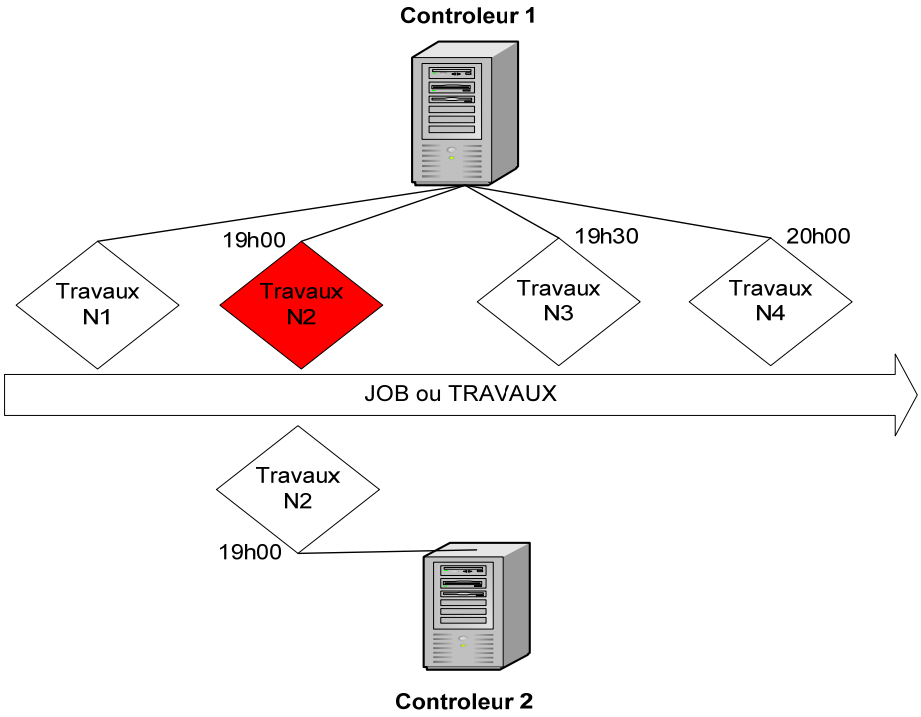


Figure 22 : Principe d'une supervision redondante

Ce scénario permettrait la continuité de la supervision en cas de défaillance du serveur superviseur principal. Ce scénario n'est pas implémenté chez AXA. Il pourra être mis en œuvre avec l'évolution de la supervision.

III.4.2 La fiabilité de la supervision

La supervision a été réalisée afin de générer le moins de tickets d'incidents non pertinents. Les algorithmes permettent une double vérification lors de chaque test en cas de détection d'une anomalie ou d'un incident. Cette double vérification permet de s'assurer que l'incident n'est pas lié à une microcoupure réseau entre les différents contrôleurs de domaines.
En effet, il est courant d'avoir des « mini-coupures » réseaux pouvant aller jusqu'à plusieurs dizaines de secondes entre plusieurs liens de l'architecture réseau de l'entreprise.
Bien que toutes les mesures aient été prises, il peut arriver que la supervision génère des incidents qui soient résolus sans intervention des équipes techniques. Ce phénomène est très connu mais reste très marginal. Il peut être dû à une défaillance d'un service concerné par les tests de supervision. Lors que cette défaillance survient, Windows peut relancer le service si les options de récupérations ont été définies, voir figure 23.
Les tests de supervision réalisés au moment de la défaillance, seront donc validés en incident durant les plages de service. Mais lorsque les équipes techniques vérifieront l'état du contrôleur de domaine, le système aura probablement déjà relancé le service concerné.
Dans ce cas précis, la supervision aura joué son rôle.

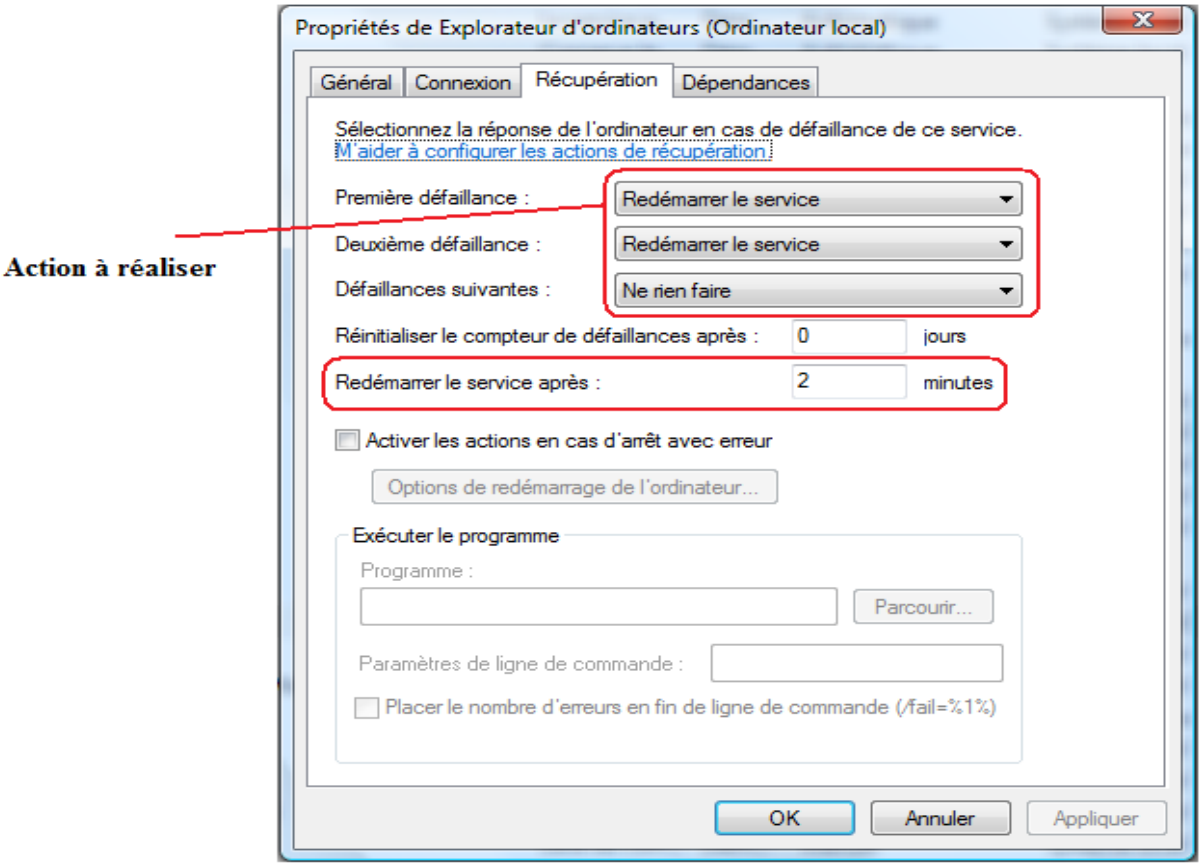


Figure 23 : Récupération automatique des services

Depuis la mise en place de la supervision Active Directory, de nombreux incidents majeurs ont ainsi été évités.
L'architecture technique réseau peut engendrer de la latence, ce qui peut impacter les performances de la supervision.

III.4.3 Les problèmes de performance

Les problèmes de performances sont connus sur tous les outils de supervisions du marché. Ces problèmes sont plus fréquents sur les supervisions sans agents et couvrant des réseaux étendus avec de faibles bandes passantes. Il existe quatre causes principales causant des problèmes de formances :

- **La latence réseau :**
  La latence est le temps que met paquet pour aller d'un point A (la source) à un point B (la destination). Plus ce temps est important et plus il y a de la latence. Lorsqu'un paquet est envoyé sur le réseau, il peut traverser des équipements ayants des débits différents. C'est le cas des sites en régions connectés en liaison spécialisées aux sites principaux d'AXA de Clichy et de Lognes. Lorsqu'une commande envoyée par la supervision d'un point A vers le point B, le temps de réponse est approximativement égal à la somme :
    - Du temps mis par la commande pour aller du point A vers le point B
    - Du temps de traitement de la commande au point B
    - Du temps de retour du traitement de la commande du point B vers le point A
    - Du temps de reconstitution de la réponse reçue (négligeable)

- **Le timeout des commandes :**
  Le « timeout » est le temps laissé à une commande pour s'exécuter avant de s'interrompre. Il correspond au délai d'expiration de la commande, s'il n'y a pas de réponse sur le système distant par exemple. Le timeout est généralement défini dans les paramètres de la commande à exécuter et peut ne pas être modifié. Il est un comportement normal dans le fonctionnement des programmes. Il sert à palier aux latences importantes sur les réseaux. Le timeout peut aller jusqu'à plusieurs dizaines de secondes pour une commande.

- **La programmation linéaire**
  La programmation linéaire est utilisée afin de s'assurer que les instructions en cours sont terminées avant d'exécuter les instructions suivantes.
  Les instructions sont mises en files d'attentes et leurs exécutions dépendent du temps d'exécution des prédécesseurs. La programmation linéaire subit fortement les effets de la latence et du timeout.
  Des solutions sont possibles, mais nécessitent des modifications importantes sur la supervision :
    - Passage en mode multitâche

- **Le nombre de contrôleurs de domaine inaccessibles à superviser**
  Les performances de la supervision peuvent être affectées par le nombre de contrôleurs de domaine à superviser injoignables par le serveur superviseur. Les contrôleurs de domaine inaccessibles amplifient le phénomène de timeout au niveau de la supervision. Ce phénomène est visible sur tous les systèmes de supervision du marché. Des solutions existent, mais uniquement pour réduire les timeout, mais ne peut en aucun cas les supprimer.

Des évolutions de la supervision seront nécessaires pour une meilleure gestion des fichiers de journalisation. Ces fichiers contiennent tous les historiques des tests de la supervision.

III.4.4 Archivage automatique de l'historique

La supervision génère des fichiers de journalisation. Ces fichiers servent d'historique pour tracer les incidents détectés par la supervision. Ces fichiers ont une durée de rétention infinie, c'est-à-dire que sa taille augmentera indéfiniment.
L'historique des données de la supervision permet de faire des statistiques sur les contrôleurs de domaine. Il sert à détecter les serveurs les plus instables, par exemple. La recherche d'information dans le fichier historique est simplifiée en utilisant les outils de bureautiques classiques du type tableur : Microsoft Excel. Mais à mesure que les données sont collectées, le volume des fichiers historiques augmente. La limite du nombre d'enregistrements à traiter par les tableurs peut être vite atteinte.
L'archivage des fichiers de journalisation ou fichier historique, permettrait un découpage comme un index. L'archivage automatique pourrait être fait selon plusieurs critères

- Annuel
- Taille du fichier historique
- Nombre d'enregistrements
- Etc.

L'archivage des fichiers historique n'a pour but que de faciliter le traitement de l'information et la gestion de l'espace de stockage de ces données. Il n'affecte pas les performances de la supervision.
Cette évolution devrait être intégrée par les équipes d'ATS en charge de la gestion de l'active directory. Des salariés d'ATS ont été formés sur la supervision active directory afin de déployer la supervision sur l'ensemble des domaines et d'apporter des améliorations futures.

III.5 Le transfert de compétences

Le transfert de compétences est une étape importante dans le cycle de vie d'un projet. Il marque la fin du projet. Quelques membres de l'équipe en charge de l'active directory seront formés pour la gestion de la supervision. Les livrables seront fournis afin d'être déployés sur de nouveaux domaines.

III.5.1 Le déploiement de la supervision

Le déploiement de la supervision est la mise en production de scripts et programmes nécessaire à son bon fonctionnement. Les scripts et programmes constituent les exécutables de la supervision.
Afin de déployer la supervision, un contrôleur de domaine superviseur a été désigné pour chaque domaine. Le rôle du serveur superviseur est détaillé au paragraphe III.3.3.
Le déploiement se déroule en 3 phases :

- **La copie des exécutables sur le serveur superviseur**
    - Tous les exécutables sont copiés aux même emplacements sur tous les serveurs superviseurs : Exemple : C:\PACKAGE_SUPERVISION
    - Il y a une cinquantaine de serveurs superviseurs
    - Ne nécessite aucune installation

- **La modification des fichiers de configuration sur chaque serveur superviseu**r
    - Personnalisation de la supervision

- **La création des travaux dans l'ordonnanceur TWS**
    - Planification des travaux pour l'ensemble des serveurs superviseurs.

La création des flux de travaux est détaillée au paragraphe IV.2. L'activation des travaux dans l'ordonnanceur permet démarrer les cycles de supervision. Les tickets d'incidents pourront alors être créés. Une formation est nécessaire pour la gestion de la supervision.

III.5.2 La formation pour déléguer la supervision

La formation sur la supervision permet de rendre autonome les membres de l'équipe en charge de l'active directory. Les différents aspects techniques sont abordés lors des différentes sessions de formation.
La formation s'est étalée sur plusieurs jours avec en moyenne une heure par jour afin de permettre de bien assimiler les différents points techniques.
Deux membres de l'équipe d'exploitation ont été formés. Le but de la formation est de déléguer la gestion complète de la supervision sur l'ensemble des domaines :

- 30 domaines de production ➔ 30 serveurs superviseurs
- 20 domaines de pré-production ➔ 20 serveurs superviseurs

Lors de la formation, les différents fichiers sources et programmes sont fournis au client.

III.5.3 Livraison des codes sources et programmes

Les codes sources et programmes nécessaires au fonctionnement de la supervision constituent les livrables. Ils seront restitués aux membres de l'équipe en charge de l'active directory.
Ces livrables permettent de superviser les nouveaux domaines active directory qui seront créés chez ATS. Les codes sources sont les bases de la supervision et serviront pour les évolutions de la supervision. La base des codes sources est composée en majorité de code Visual Basic. Le code source pourra être remplacé par tout autre langage de programmation utilisant des API. Les API ont été présentées au paragraphe II.3.1.1, et dans le tableau 5.
Les livrables sont composés d'un répertoire principal et d'une arborescence de sous répertoires comme illustré à la figure 24

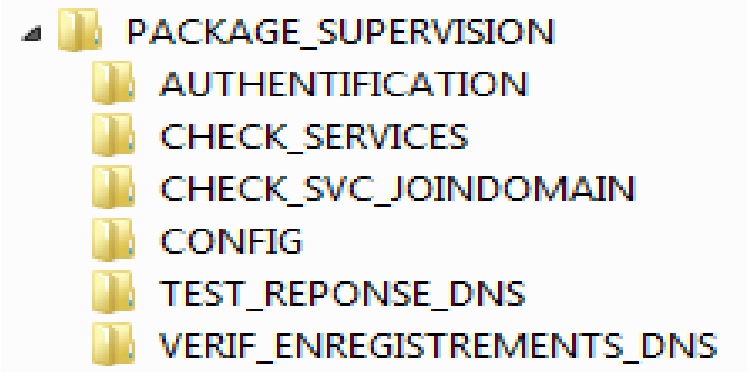


Figure 24 : Structure des dossiers de la supervision

La structure des répertoires devra être respectée afin que la supervision fonctionne correctement. Il ne faudra donc en aucun cas modifier les noms de ces répertoires ou des fichiers fournis

III.6 La supervision dans l'entreprise

L'active directory est un service d'annuaire d'entreprise fonctionnant sur les systèmes d'exploitation Microsoft Windows orientés serveurs. Les serveurs hébergeant l'active directory sont appelés « contrôleur de domaine ». L'active directory constitue un élément essentiel de l'architecture du système d'information de l'entreprise. Il permet d'accéder aux ressources de l'entreprise.

Les entreprises proposent de plus en plus de services nécessitant une connexion à l'active directory. Il est devenu au fil des années un point très critique pour les entreprises. Des incidents ou des disfonctionnements sur cet annuaire peuvent perturber le fonctionnement de l'entreprise, voire même la paralyser.
Les utilisateurs sont de plus en plus exigeants et attendent de la direction des systèmes d'information (DSI) des moyens informatiques fiables et performants. Le système d'information doit répondre aux exigences des utilisateurs. La DSI doit sans cesse innover pour proposer un service de qualité tout en composant avec la réduction des coûts imposée par la direction générale et les actionnaires.
Certains services proposés par le groupe AXA sont disponibles 24/24 et 7j/7j rendant ainsi l'infrastructure informatique très critique. Les incidents sur l'infrastructure informatique doivent être réduits afin d'éviter de perturber les activités de l'entreprise.

L'active directory est un composant sensible de l'infrastructure informatique de l'entreprise. La supervision de l'active directory est la surveillance de cet annuaire et des composants nécessaires à son bon fonctionnement. Le rôle de la supervision est d'alerter les équipes d'exploitation en cas d'apparition d'une anomalie ou d'un incident.
AXA Tech a privilégié les alertes par courriel et l'ouverture automatique de tickets de suivi des incidents dans une base centralisée de gestion des incidents. Les incidents sont référencés pour un meilleur suivi. Ils serviront pour communiquer les informations pertinentes aux équipes et aux utilisateurs concernés. AXA Tech joue le jeu de la transparence en cas d'incident sur son infrastructure informatique.

La supervision de l'active directory teste à intervalle régulier les composants indispensables à son bon fonctionnement. Les résultats de ces contrôles permettent d'établir une cartographie de l'état du service d'annuaire et de ses composants. L'historique des tests réalisés par la supervision est sauvegardée afin d'être exploité ultérieurement. La supervision permet aux équipes d'exploitation d'être plus réactives. Ainsi, les incidents sont traités avant sa détection par les utilisateurs.

La supervision de l'active directory utilise les composants de base de Microsoft Windows. Certains outils utilisés sont disponibles gratuitement sur le site de Microsoft, l'éditeur du système d'exploitation. La planification d'exécution de la supervision est réalisée par l'ordonnanceur déjà en place chez AXA Tech, ce qui permet une gestion centralisée.

IV Conception de la supervision

La conception de la supervision de l'active directory ou d'un système informatisée n'est pas réservée qu'aux grands éditeurs de logiciels. Il est possible de concevoir une supervision fiable et efficace sans budget.
La connaissance de l'environnement à superviser est indispensable. La supervision ne doit pas s'arrêter aux contrôles de l'état de fonctionnement des équipements ou des systèmes d'informations, mais doit s'inscrire dans la politique globale de l'entreprise.
Les étapes de la réalisation de la supervision seront abordées afin de fournir les bases nécessaires. La réalisation d'un outil de supervision nécessite quelques notions de programmation logicielle ou système.
L'exécution de la supervision est planifiée par l'ordonnanceur TWS. Il peut être remplacé n'importe quel ordonnanceur ou planificateur de taches. La création des flux de travaux dans l'ordonnanceur TWS sera présentée avec une vision purement technique.

IV.1 Les étapes de la conception

La conception de la supervision est une étape décisive dans la réalisation du projet. Les composants qui seront utilisés pour la supervision devront respecter les exigences d'ATS.

IV.1.1 La recherche des éléments à superviser

La recherche des éléments à superviser est faite durant la phase de l'étude des tickets d'incidents historiques. Les incidents sur l'infrastructure d'AXA sont référencés dans la base des incidents. La recherche des incidents permet d'identifier les points faibles du système.
Les informations saisies dans chaque ticket d'incident doivent être pertinentes afin d'être exploitées ultérieurement. La qualité des informations permet de gagner du temps dans la compréhension et l'origine de l'incident.

IV.1.1.1 La recherche d'incidents par critères

La recherche des incidents est exclusivement basée sur les incidents consignés dans la base de gestion des incidents et sur les communications faites relatives aux incidents.

- **Recherche par mots clés**

Le logiciel de gestion des incidents permet des recherches par mots clés. Le choix des mots clés pour la recherche des incidents est important. AXA a fait le choix de standardiser le nom de ses serveurs. Bien que ce ne soit pas le cas pour tous les domaines, car historiques, la plus part des contrôleurs de domaine respectent la nomenclature ci-dessous.

- **Les serveurs de production**
  - **PRINTXXDCYY** ➔ **PRINTSIEGDC5**
    - **PRINT :** environnement de production
    - **XX** : une partie ou la totalité du nom du domaine.
    - **DC** : Domain Controller ➔ Contrôleur de domaine en français
    - **YY** : l'identifiant du contrôleur

La recherche des incidents dans la base des incidents est facilité une nomenclature standardisée. L'utilisation de caractères « joker » augmente les possibilités de la recherche. Les contrôleurs de domaines de tous les domaines seront représentés sous la forme : **%DC%**. Si des serveurs non contrôleurs de domaine comportent « DC » dans leur nom, il faudra les exclure lors de l'analyse des résultats. La figure 25 est le résultat de la recherche des incidents avec le critère nom des serveurs contenant « **DC** ».

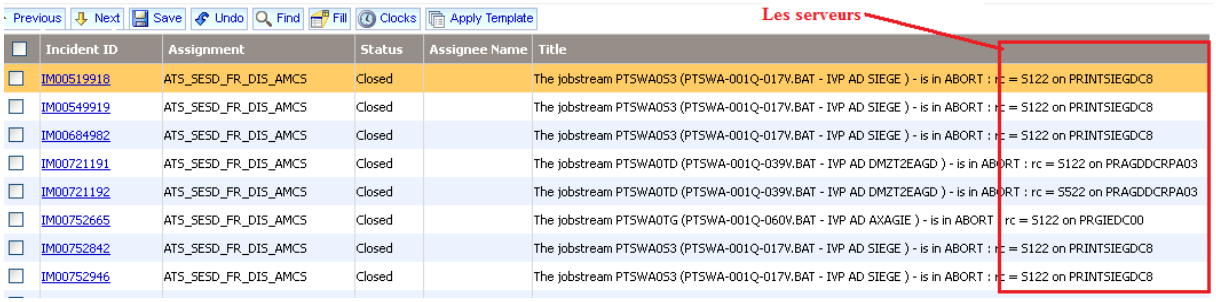


Figure 25 : Résultat de recherche d'incidents

La recherche par mot clé ne s'arrête pas uniquement au nom des serveurs. Le but n'est pas de fournir une liste complète des mots clés, car ils dépendent de la saisie des informations par l'opérateur dans la base des incidents. La qualification d'un incident initialement constaté pour un seul utilisateur peut évoluer. L'incident peut affecter de nombreux utilisateurs.

- ## Recherche par criticité

La recherche d'incidents par criticité permet de faire un premier tri. Les incidents de priorité P1, décrits dans le paragraphe II.2.2, sont des incidents dont les conséquences sont les plus importantes. On peut ainsi supposer que ces incidents ont affecté de nombreux utilisateurs. La criticité ne fournira pas la liste d'incidents à analyser, mais l'ensemble des incidents correspondants à ce critère de recherche. Des filtres supplémentaires devront être combinés à cette recherche afin d'avoir le moins de trie manuel par la suite. La combinaison de la recherche par criticité avec la recherche par mot clé fournit une base de travail :

- Recherche par mot clés : %DC%
- Criticité : P1% ou P2%

Ces recherches peuvent être sauvegardées comme indiquées dans la figure 26.

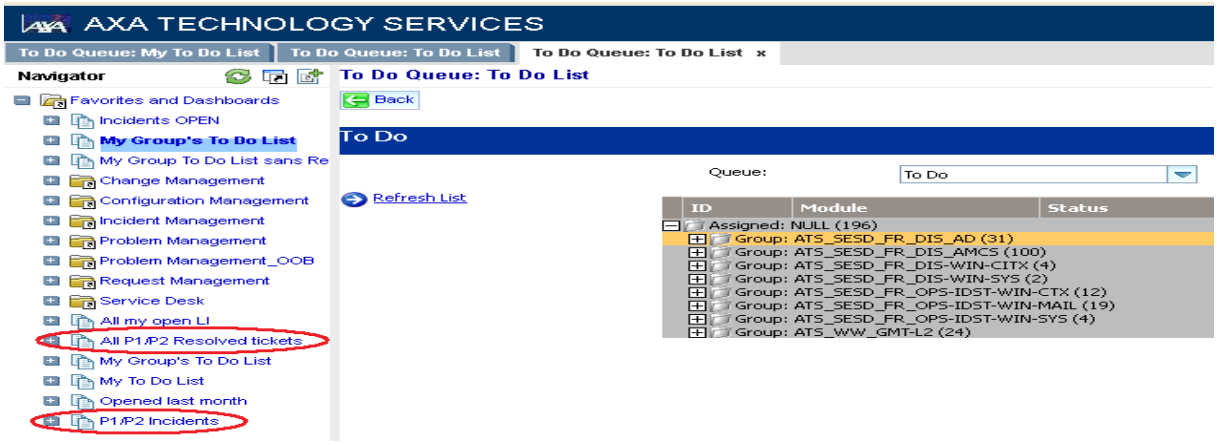


Figure 26 : Recherche d'incident par priorité

Les incidents créés dans la base par les opérateurs devront être bien renseignés afin de faciliter les recherches. Les équipes d'exploitation sont responsables de requalifier les incidents en changeant la priorité si besoin. Ce changement de critère est important, car il permet de mieux exploiter les informations dans la base.

- **Recherche par date**

La recherche des incidents par date n'est pertinente que si elle est combinée avec les autres critères de recherches cités ci-dessus. Cette recherche est néanmoins importante, car elle permet un filtre directement dans l'application de gestion des incidents ce qui évite un trie manuel des résultats.
Il est ainsi possible de ne rechercher que les incidents constatés durant l'année 2012, si l'on considère que les incidents antérieurs n'ont pas d'intérêt du point de vue technique. Si l'ensemble de plateformes matérielles des contrôleurs de domaine a été remplacé en 2011, et les systèmes d'exploitation réinstallés. Les incidents survenus avant 2011, n'ont plus grand intérêt. Car les résultats de la recherche pourraient conduire à des investigations qui ne seraient plus d'actualités.

- **Recherche dans les historiques des communications sur les incidents**

Tous les incidents dont la priorité est P1, font l'objet d'une communication par courriel à l'ensemble des équipes techniques. La priorité des incidents est décrite au paragraphe II.2.2. Il existe un modèle de document utilisé pour la communication par courriel.
La recherche des incidents dans l'application de gestion des courriels fournit la liste des communications sur l'ensemble des incidents.
Il n'y a pas de communications sur les incidents de faibles priorités. Un incident avec une faible priorité n'est pas forcément un incident sans gravité. Il a peut être été détecté et corrigé avant que les conséquences ne soient visibles.
La figure ci-dessous est l'interface de recherche des communications dans l'application de gestion des courriels.

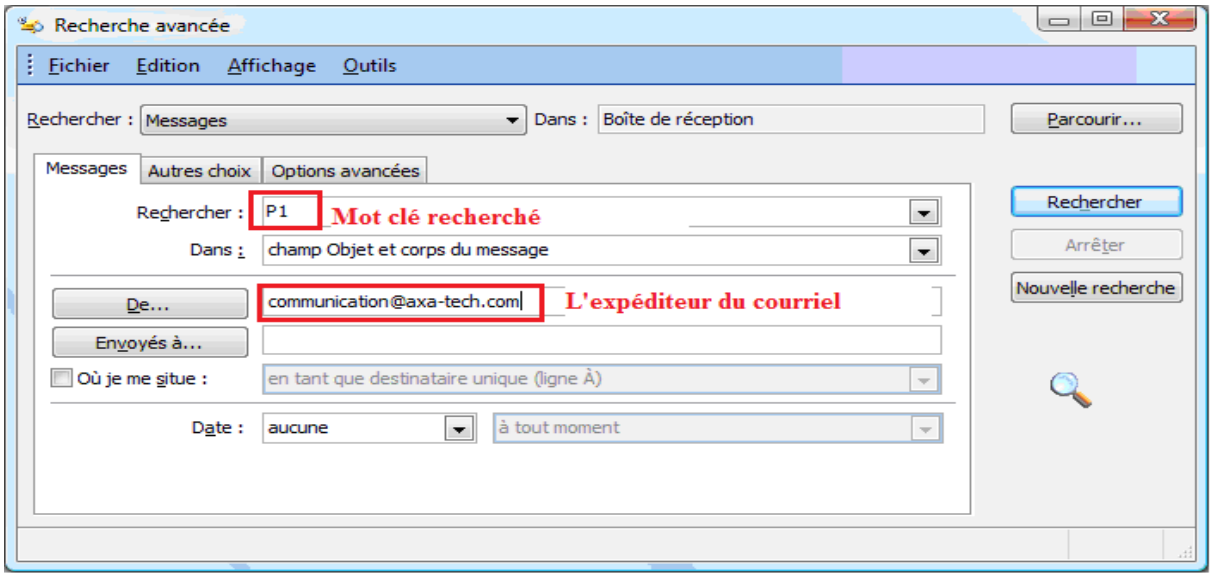


Figure 27 : Recherche des communications sur les incidents

La recherche doit donc s'étendre à tous les moyens de collectes des informations relatives aux incidents.

IV.1.1.2 Le retour d'expérience

La base des incidents regorge d'informations importantes. Elle permet connaître l'exploitant qui est intervenu pour résoudre chaque incident. Elle trace les actions et escalades du ticket d'incident.
L'audition des exploitants pourra apporter des informations précieuses. L'exploitant fournira les informations dont il dispose et précisera si cet incident aurait pu être détecté. Ces auditions ont permis d'avoir des informations précieuses sur l'origine de certains incidents.

- Il a été constaté dans certain cas que des services Windows étaient arrêtés sur un contrôleur de domaine, alors qu'il y avait une routine de redémarrage automatique du service en cas d'arrêt. La vérification du service dans le gestionnaire de service ou avec les commandes systèmes a permis d'identifier le problème. Pour résoudre l'incident, le service concerné a simplement été démarré.
  - ⇒ **Etablir la liste des services à superviser**
  - ⇒ **Tester ces services**

- De même, des services ne répondaient pas aux requêtes faites par les utilisateurs alors qu'ils étaient démarrés. C'est le cas du service DNS, qui ne répond pas aux requêtes des DNS. L'identification du problème peut se faire en ligne de commande, avec la commande « nslookup ».
  - ⇒ **Tester la résolution de noms DNS**

- L'incident le plus pénalisant intervient lorsque les utilisateurs n'arrivent pas à se connecter sur leurs stations de travail. Ils n'ont plus accès à leur environnement de travail comme illustré à la figure 28. L'identification du contrôleur de domaine qui est inopérant s'avère fastidieux. Il faut se connecter sur chaque contrôleur du site concerné. La notion de site est décrite au paragraphe II.3.1.1. Une autre solution consiste à utiliser une application ayant une API pour se connecter à l'active directory, comme l'outils de gestion de l'active directory. On se connecte sur chaque contrôleur de domaine à tour de rôle jusqu'à ce qu'il soit identifié. Cette méthode est fastidieuse dans de vastes domaines.
  - ⇒ **Tester l'authentification sur l'ensemble des contrôleurs de domaines**

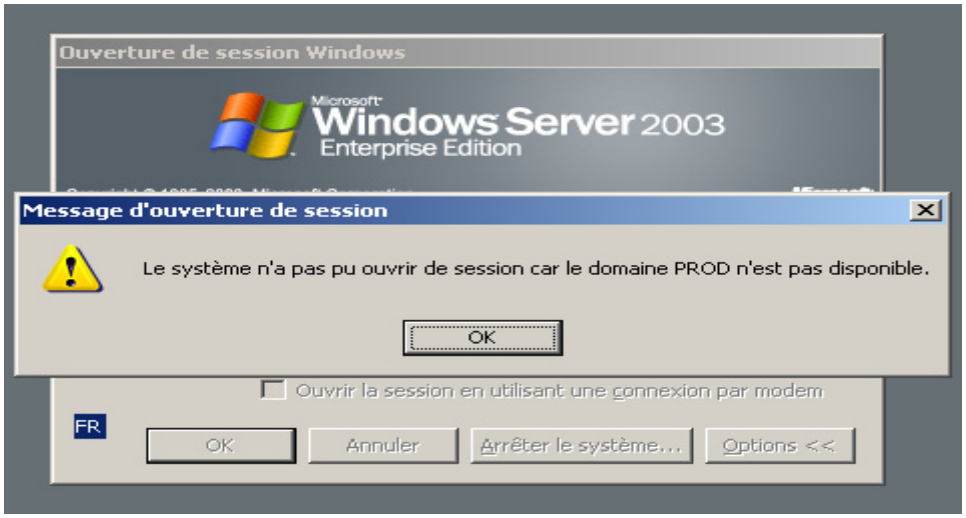


Figure 28 : Incident de connexion à Windows

IV.1.1.3 La connaissance des systèmes à superviser

L'analyse des informations ainsi collectées a permis d'identifier d'autres sources d'incidents pouvant générer des incidents majeurs. La connexion à certaines ressources de l'entreprise nécessite une résolution de nom DNS. Certaines de ces ressources sont accédées par des centaines ou des milliers d'utilisateurs. Lorsque le nettoyage automatique des enregistrements DNS est activé, des incidents majeurs peuvent se produire dans certain cas. La fonction de purge automatique est un mécanisme intégré dans le DNS Windows.
Le nettoyage automatique intervient 14 jours après la dernière modification de l'enregistrement. Le nettoyage ne concerne que les enregistrements créés dynamiquement par l'équipement. Durant 7 jours, l'équipement ne peut pas modifier l'enregistrement qu'il a créé dans le DNS, on parle d'« **intervalle de non actualisation**». A partir du 7è jour et jusqu'au 14è jour suivant la dernière modification de l'enregistrement dans le DNS, l'équipement peut modifier cet enregistrement. Cette période comprise entre le 7è et le 14è jour est appelée « **intervalle d'actualisation** ». Si aucune modification ou mise à jour n'intervient pendant l'intervalle d'actualisation, et que le nettoyage est activé, l'enregistrement sera supprimé sur l'ensemble des DNS du même domaine. Les requêtes DNS pour résoudre le nom de cette ressource ne renverront pas d'adresse IP.

⇒ **Etablir la liste des enregistrements critiques**
⇒ **Vérifier les enregistrements critiques dans le DNS**

La figure 29 fournit les valeurs par défaut pour le nettoyage des enregistrements. Bien que ces valeurs puissent être modifiées, il n'est ce pendant pas recommandé de modifier ces valeurs pouvant impacter l'active directory.

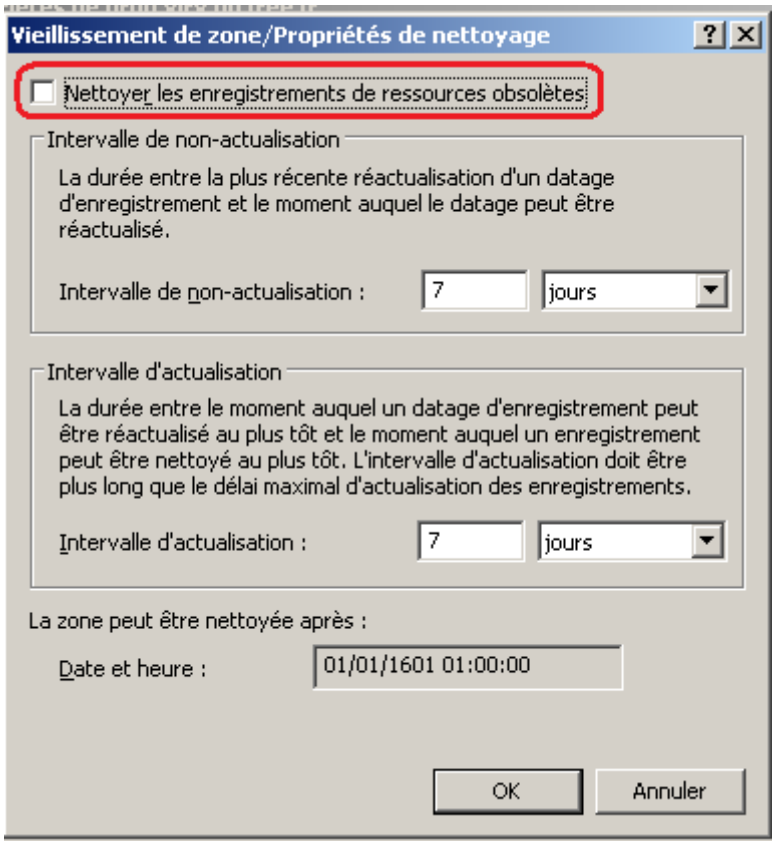


Figure 29 : Nettoyage des enregistrements dans le DNS Windows

IV.1.2 L'étude de faisabilité

Les exigences d'ATS sur le choix les outils à utiliser, m'ont contraint à rechercher des solutions qui embarquent des outils natifs à Windows. L'étude des incidents, présentée au paragraphe IV.1.1.1, a permis d'établir les éléments à superviser sur les contrôleurs de domaine.

- **Tester l'authentification**

Il existe des API qui permettent de se connecter à l'Active directory et d'interagir avec les objets, décrit dans le tableau 5. Ces API permettent de tester que le couple compte utilisateur et mot de passe sont validés par un contrôleur de domaine. Les API existent pour les langages de programmations le Visual Basic Script. Il sera donc possible de les exploiter sans utiliser d'outils tiers, et répondre aux exigences d'ATS. Ces API sont utilisées pour réaliser des taches d'administration système, mais rarement utilisées pour réaliser la supervision. Le test de faisabilité consiste à tester un compte et le mot de passe associé. Si la commande retourne une erreur, elle sera interprétée et traduite en anomalie. Sinon, le test est validé.

- **Tester les services**

La supervision des services consistera à vérifier que le service est dans l'état « démarré ». Des commandes existent sur Microsoft Windows pour vérifier l'état d'un service localement ou sur un système distant. L'interrogation des services se fait à l'aide de la commande « **SC** », pour « Service Control » ou Contrôle de Service en français. La syntaxe de la commande est la même pour toutes les versions de Windows. Cette commande fait partie des commandes basiques utilisées pour les taches d'administration courantes sur des ordinateurs Microsoft Windows.

- **Etablir la liste des services à superviser**

  Les contrôleurs de domaine ont presque tous les mêmes rôles, l'active directory est un annuaire distribué entre les contrôleurs de domaine. Les services sont à quelques exceptions près les mêmes sur tous les contrôleurs de domaines. Les services sélectionnés sont nécessaires au bon fonctionnement du système et de l'active directory.

  La liste des services à superviser a été faite en se basant sur tous les services démarrés sur plusieurs contrôleurs de domaine ne présentant aucunes anomalies. Les services ont été ensuite analysés afin de ne garder que ceux qui ont un rôle important.

- **Tester la résolution de noms DNS**

Le test de résolution de noms DNS est une opération courante souvent utilisée par les administrateurs et ingénieurs système. Ce test permet d'interroger à distance ou localement un serveur DNS. Il existe plusieurs commandes qui permettent de vérifier l'état la résolution de noms sur un serveur DNS. La commande qui a été retenue est « NSLOOKUP ». Il faut réaliser les tests de résolution de nom DNS, mais sur quel enregistrement ? L'idée est d'innover et de proposer une solution efficace et fiable.

Les enregistrements dans le DNS sont amenés à disparaître, donc le choix de l'enregistrement à tester doit être stratégique. Le nom de domaine possède des enregistrements DNS avec une durée permanente. La vérification de ces enregistrements servira à valider l'état du service DNS. Ces enregistrements seront les derniers supprimés si le nom de domaine devait disparaître à son tour. C'est donc un choix très judicieux d'utiliser le nom de domaine pour interroger le serveur DNS.

- **Vérifier les enregistrements critiques dans le DNS**

La suppression des enregistrements critiques peut engendrer des incidents majeurs. La vérification de la présence de ces enregistrements permet de s'assurer que les ressources sont toujours accessibles par l'ensemble des utilisateurs.
Des tests de faisabilités ont été effectués avec commande « NSLOOKUP ». Ces tests n'ont pas été concluants. Si le nombre d'enregistrements à tester est important, le timeout sera aussi important si le contrôleur de domaine est inaccessible. La timeout a déjà été abordé au paragraphe III.4.3. Dans le cas de la commande « NSLOUKUP », le time out par défaut est de 2 secondes. Avec uniquement 30 enregistrements, le timeout sera d'une minute. Durant une minute, le système attendra sans pouvoir exécuter d'autres instructions.
La solution a été trouvée dans les outils proposés par Microsoft sur son site internet. L'utilitaire « **DNSCMD** » permet d'extraire tout le contenu du serveur DNS. Le contenu est exportable sous un format texte. Le texte sera ensuite analysé pour extraire les informations recherchées. Lors des tests de faisabilité avec l'utilitaire « DNSCMD », les extractions ont durée moins de 10 secondes pour plus de 10 000 enregistrements dans le DNS.

- **Etablir la liste des enregistrements critiques**

La liste des enregistrements a été faite en se basant sur les incidents constatés dans la base des incidents, en accord avec le responsable du service, Olivier MANZANO. Les enregistrements concernent les serveurs de stockage en réseaux, connus sous le nom de NAS (Network Attached Storage en anglais).

A ce stade du projet, je sais seulement qu'il est possible de tester chaque contrôleur de domaine de manière unitaire. La conception de la supervision est envisageable car techniquement j'ai tous les outils nécessaires.

IV.1.3 Un concept novateur

L'idée principale est de mettre en place une supervision à bas prix mais qui réponde aux besoins du client ATS. Plusieurs idées ont très rapidement émergées.
La conception d'une supervision portable qu'il serait facile à déployer et qui utiliserait les programmes de natifs de Microsoft Windows. Il suffirait de faire appel à ces programmes ce qui éviterait de les développer. Le programme d'installation de la supervision se présenterait comme un répertoire à copier qui contiendrait tous les scripts et codes sources nécessaire pour son fonctionnement.
La création des programmes génériques utilisables par tous les domaines. Les informations de personnalisations seraient dans les fichiers de paramétrage. Certaines informations contenues dans les fichiers de paramétrage seraient communes à l'ensemble des domaines. Ce sera par le cas par exemple pour un certain nombre de services qui sont communs aux différents domaines. Les codes sources ne seraient modifiés que pour ajouter de nouvelles fonctionnalités.
La conception de plusieurs briques dans la supervision rattachées à un programme principal, le lanceur, permettrait de tester individuellement chaque brique. Ainsi en cas de modification d'une des briques il n'y a pas de régression sur les autres briques. Dans les domaines hors production, la supervision des enregistrements dans le DNS pourra être désactivée, car il n'y a de serveur de stockage en réseaux dans tous les domaines.
L'ordonnanceur TWS permet de contrôler depuis une seule console la supervision sur l'ensemble des domaines. Il est possible d'arrêter la supervision, de la déplacer sur un autre serveur superviseur. Etc.

IV.1.4 La réalisation de la supervision

La réalisation de la supervision répond aux exigences d'ATS. La supervision est évolutive et facile à déployer.

IV.1.4.1 La modélisation

La modélisation permet d'avoir une maquette ou un schéma directeur sur ce que l'on attend du produit final. Elle doit se rapprocher le plus possible des exigences du client. Elle sert à une meilleure compréhension de chaque brique dans la supervision.

- **Modélisation du test d'authentification**

La modélisation du test d'authentification, représentée à la figure 30, décrit les différents processus à réaliser. Les deux comptes sont testés une première fois. Si les deux comptes sont en échecs sur un contrôleur de domaine, un second test sera effectué uniquement sur ce contrôleur en échec. L'initialisation de boucle est une fonction basique. Si des échecs existent, une seconde boucle sera créée, sinon elle sera inhibée.

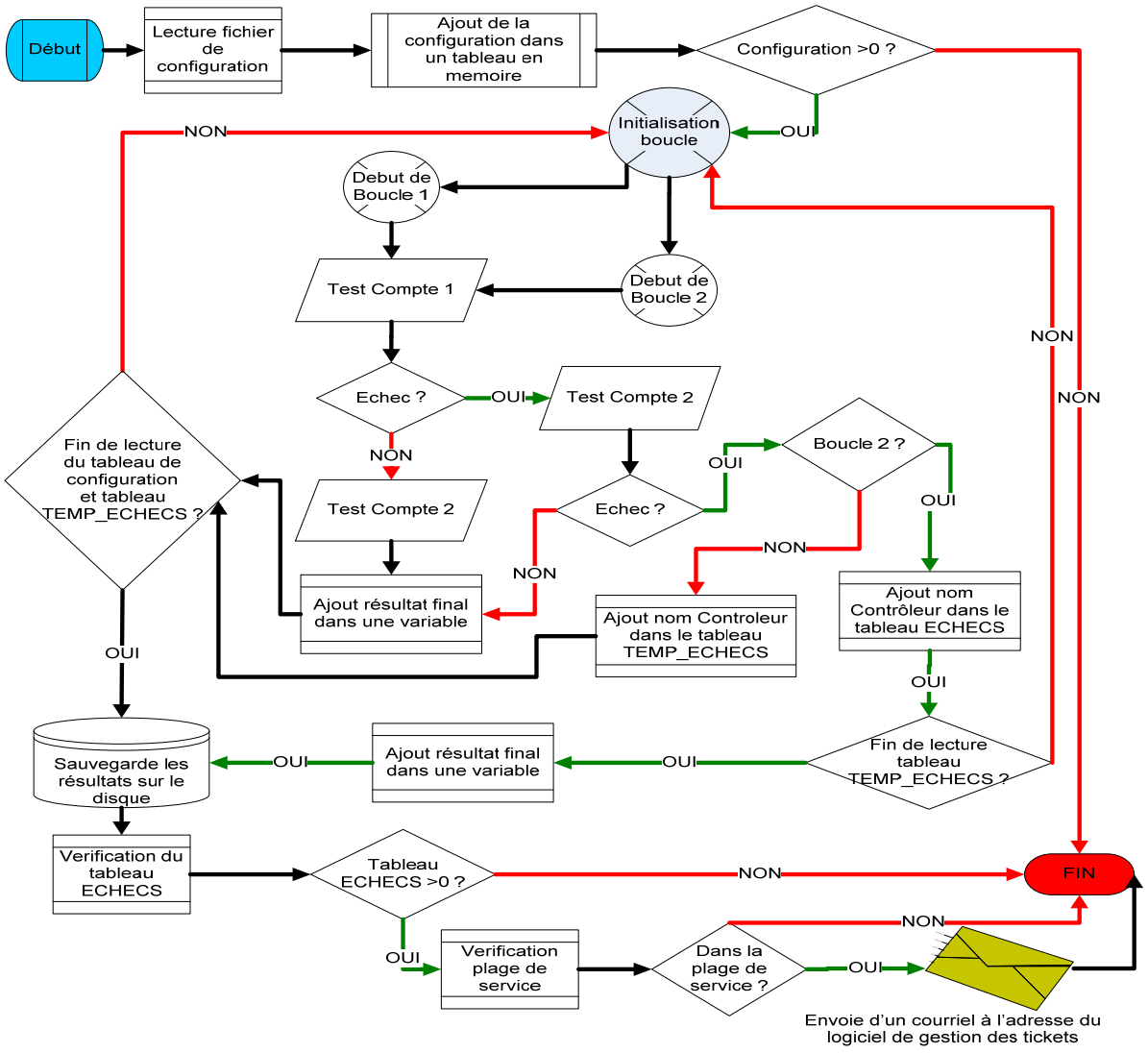


Figure 30 : Modélisation du test d'authentification

- **Modélisation du test des services**

Les tests de services sont basés sur les mêmes principes que le test d'authentification. L'état des services est testé dans un premier temps sur l'ensemble des contrôleurs. Les services qui ne sont pas en état « **DEMARRE** » seront testés lors du second test. La figure 31 illustre le mécanisme à mettre en place pour réaliser la supervision des services.

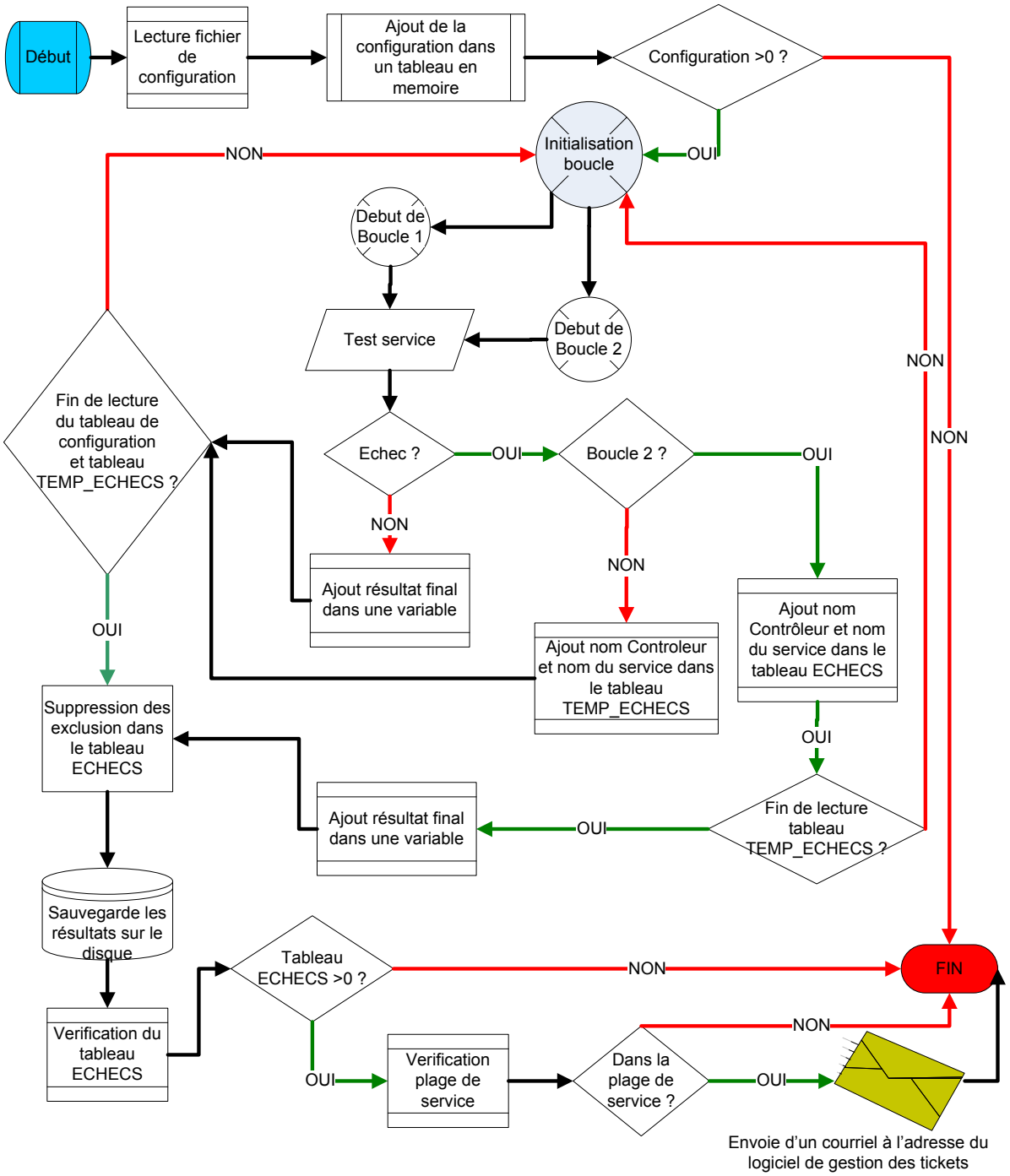


Figure 31 : Modélisation du test des services

- **Modélisation du test de résolution de noms DNS**

Les tests DNS seront réalisés sur chaque contrôleur de domaine lors du premier passage. Seuls les contrôleurs rencontrant une anomalie seront testés lors du second passage. Contrairement à la modélisation du test des services, le test DNS ne gardera que les noms des contrôleurs de domaines dans le tableau des échecs. Le nom du domaine à tester est renseigné dans les fichiers de paramétrage et reste inchangé. Le test est modélisé par la figure 32.
L'annexe 10 fournit quelques exemples de tickets de d'incidents créés par la supervision.

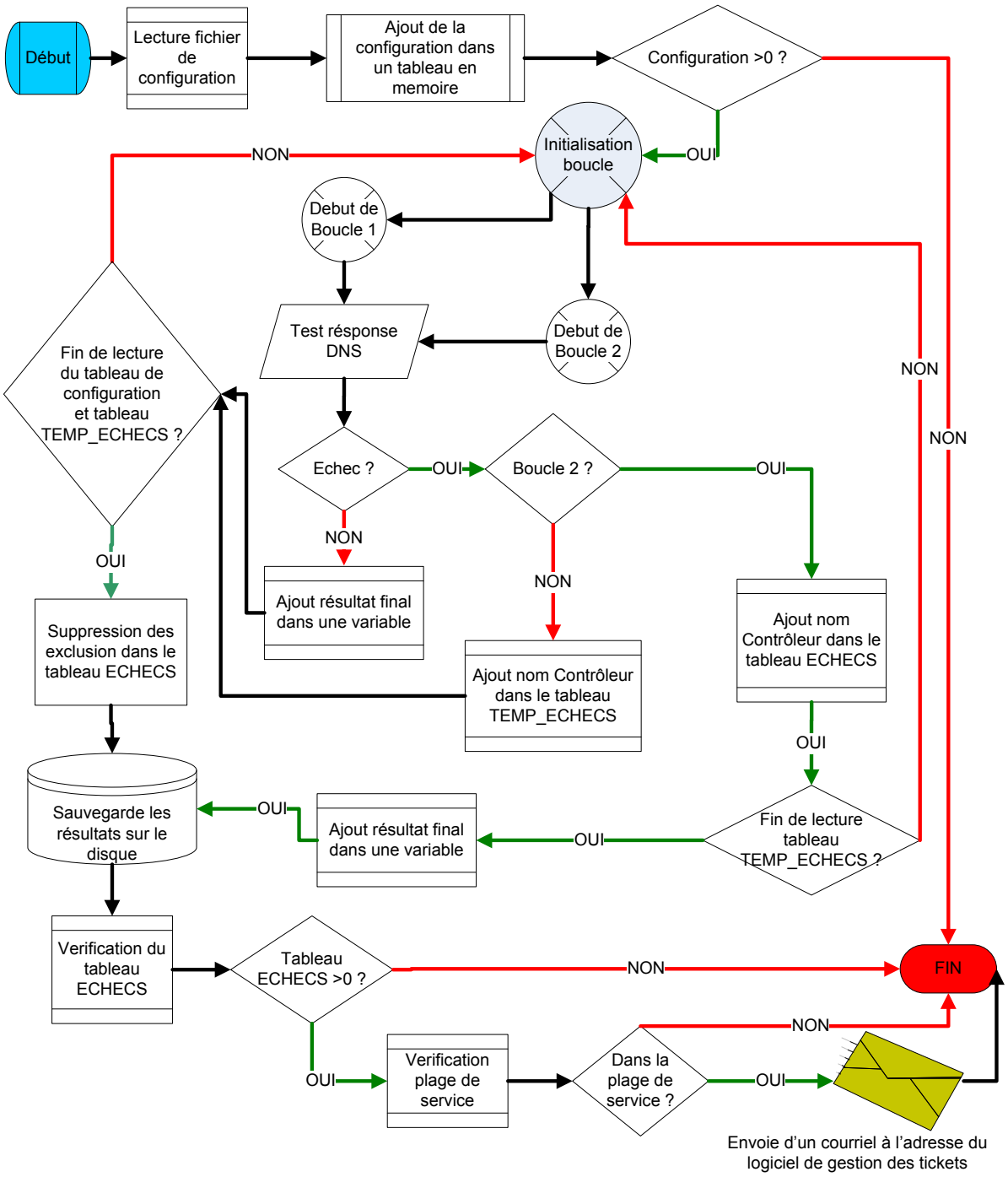


Figure 32 : Modélisation du test de résolution de noms DNS

- **Modélisation du test de vérification des enregistrements dans le DNS**

Les enregistrements contenus dans les DNS sont répliqués entre tous les contrôleurs. C'est-à-dire si un enregistrement est ajouté il sera répliqué automatiquement sur tous les autres contrôleurs ayant le rôle de serveur DNS. Il en est de même lorsqu'un enregistrement est supprimé. Il n'est donc pas nécessaire de contrôler la présence des enregistrements sur l'ensemble des contrôleurs de domaine. Lorsque le DNS fournit une réponse à un client, ce dernier garde la réponse dans une zone tampon appelé « cache DNS». La durée par défaut de l'enregistrement dans le cache est d'une heure (3600 secondes). Le test sera donc réalisé sur un seul serveur DNS. L'initialisation de boucle n'est donc pas nécessaire, car les tests sont réalisés sur le même contrôleur de domaine. Comme pour tous les autres tests, il y a toujours deux passage du test afin d'éliminer toute perturbation passagère lié à des microcoupures réseaux par exemple. La figure 33 modélise le fonctionnement qui est attendu pour ce test.

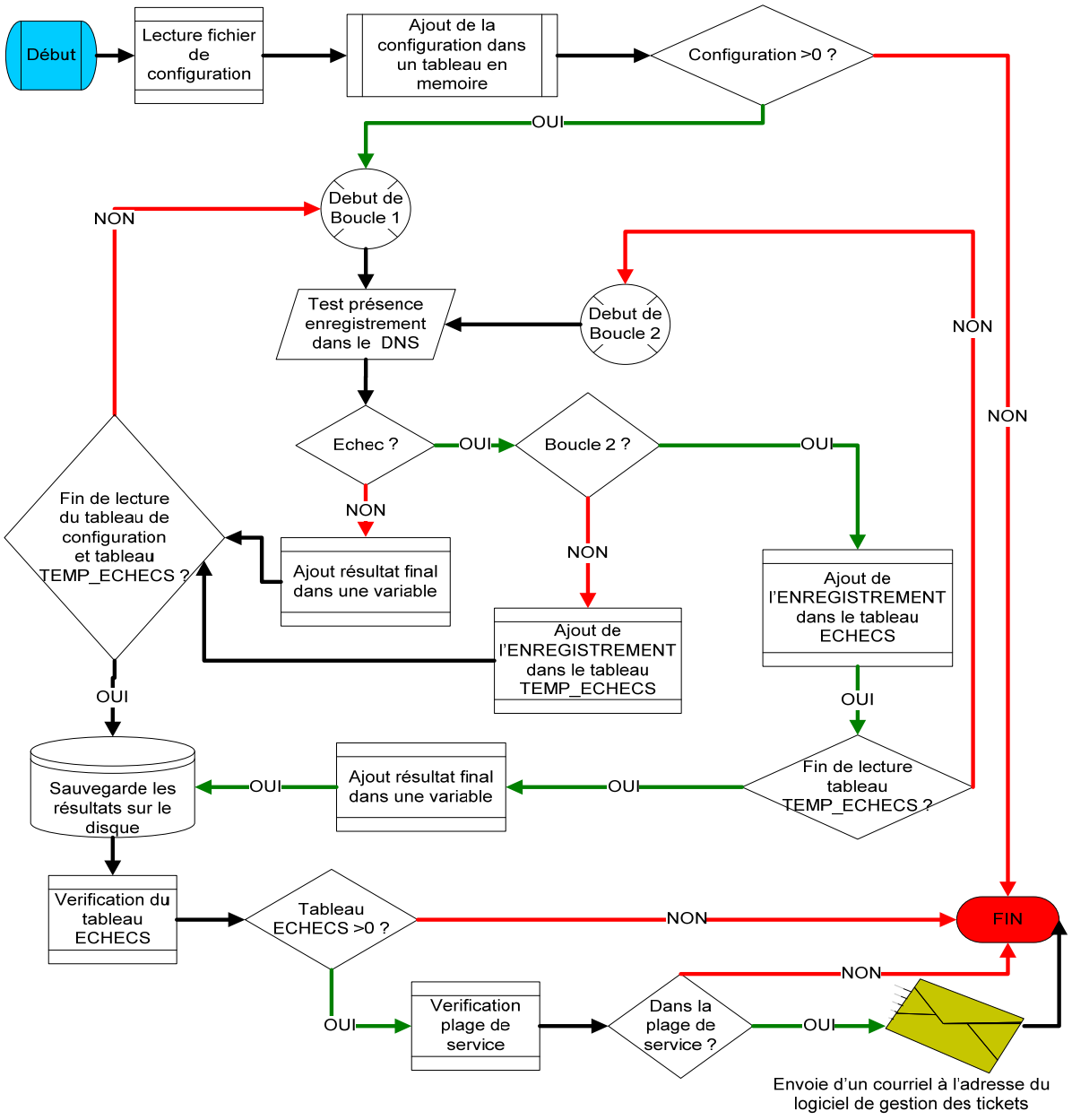


Figure 33 : Modélisation du test de vérification des enregistrements dans le DNS

- **Modélisation du test du compte d'installation des serveurs**

La modélisation du test du compte d'installation des serveurs est presque similaire de celle du test d'authentification. La seule différence c'est qu'il n'y a qu'un seul compte d'installation pour chaque domaine. Le test sera donc basé que sur le seul compte disponible pour chaque domaine. Il n'est donc pas nécessaire de reproduire la modélisation qui serait une réplique du test d'authentification.
Une option a été envisagée, en utilisant les propriétés de réplications de l'active directory. L'annuaire active directory étant distribué entre tous les contrôleurs, lorsqu'un objet est modifié sur un contrôleur (compte verrouillé par exemple), le verrouillage se propagera sur l'ensemble des contrôleurs. En utilisant cette propriété, on serait tenté de ne vérifier l'état du compte que sur un seul contrôleur de domaine. Cette solution si elle était envisagée, permettrait d'accroître les performances de la supervision mais en contrepartie nécessiterait une gestion manuelle et rigoureuse.
Lorsque le contrôleur de domaine qui est chargé de tester le compte serait hors service, la bascule de la supervision sur un autre contrôleur serait faite dans les fichiers de configuration. Cette manipulation nécessiterait une intervention d'un administrateur système. La figure ci-dessous illustre le processus de gestion d'un superviseur unique pour la supervision du compte d'installation.
Cette architecture n'a pas été retenue, car elle serait trop contraignante d'un point de vu de gestion.

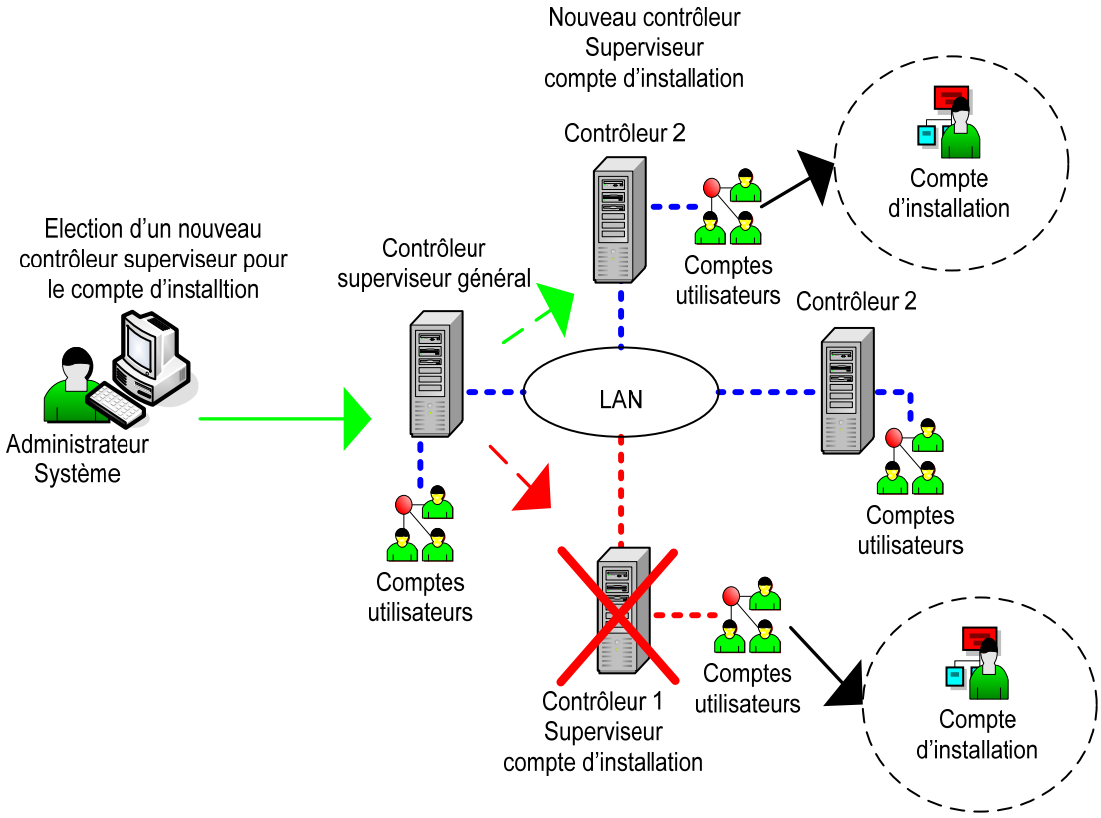


Figure 34 : Modèle d'architecture non retenu

- **Modélisation de la création de tickets de suivi des alertes**

Lorsqu'une alerte est confirmée, c'est-à-dire qu'un incident a été détecté dans la plage de service, un courriel sera envoyé à l'équipe d'exploitation et à la boite aux lettres de l'application de gestions des tickets. Ces tickets permettent de suivre l'incident jusqu'à sa résolution. Après la résolution de l'incident, le ticket de suivi servira d'archive ou de base de connaissance pour des incidents similaires. Le processus de transformation du courriel en ticket de suivi de l'incident est modélisé pour une meilleure compréhension par la figure 35.

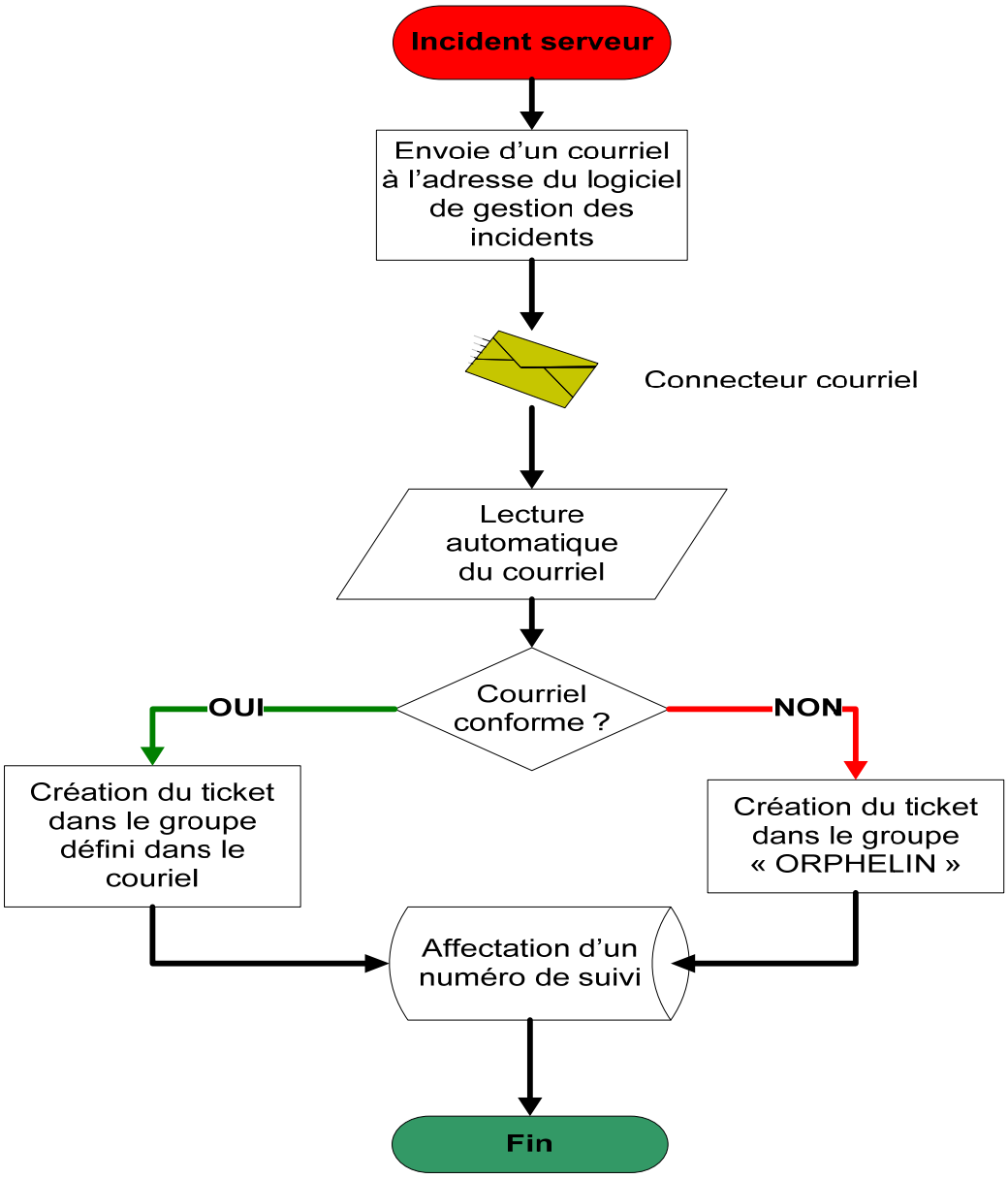


Figure 35 : Processus de création d'un ticket de suivi d'incident

- **Modélisation du lanceur**

Le lanceur est le programme principal de la supervision. Son rôle est d'exécuter les différents programmes selon un ordre défini.
L'ordonnanceur initialisera le lanceur. Ce dernier exécutera chaque programme de la supervision. Il s'assurera que le programme courant soit terminé avant de lancer le programme suivant.
Il est possible de changer le fonctionnement en exécutant le programme suivant sans attendre la fin du programme précédent. Mais dans ce cas, il n'est plus possible de gérer la fin des travaux par l'ordonnanceur. Lorsque le lanceur a terminé l'exécution de tous les programmes, l'ordonnanceur récupère le code d'exécution. Ce code d'exécution permet de déterminer si les travaux se sont bien déroulés.

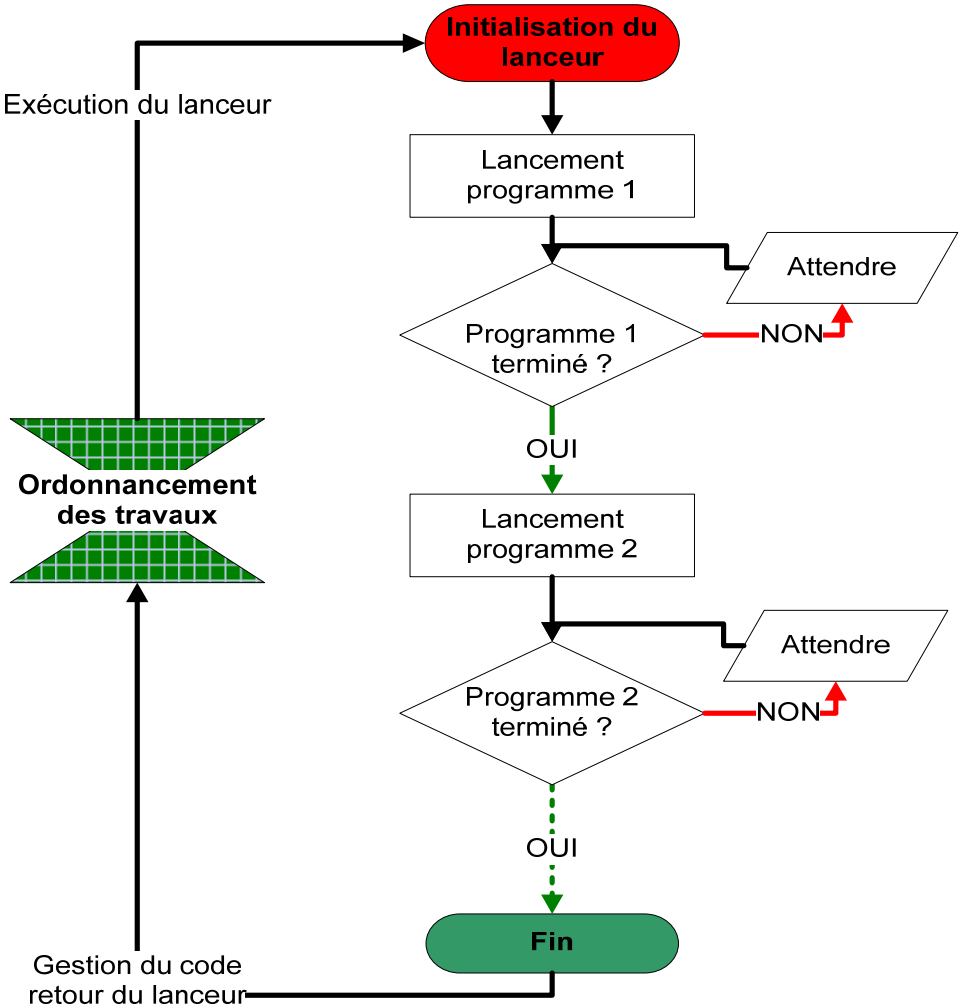


Figure 36 : Modélisation du lanceur

La modélisation de l'ensemble des briques de la supervision est terminée. La création des codes sources de la supervision consistera donc à respecter toutes les contraintes de la modélisation.
Le développement des codes sources dans le langage Visual Basic Script (VBS) nécessite quelques notions de programmation. Quelques exemples du code source sont fournis en annexe. Ils seront commentés afin de permettre une meilleure compréhension.

IV.1.4.2 Lecture automatique de la configuration

Les programmes de la supervision chargent les fichiers de configurations en mémoire. Ces fichiers ont été présentés au paragraphe III.1.4. Le principe de la lecture de la configuration est la même pour l'ensemble des programmes. La lecture des fichiers de configuration permet d'extraire automatiquement les données en fonction des mots clés qui leur sont associés. Chaque fichier de configuration est ouvert en positionnant le pointeur en début de fichier. Le pointeur de fichier est un entier long, il permet de déterminer à partir de quel octet (ou position) les opérations seront réalisées. Le pointeur de chaque fichier sera positionné en début de fichier (pointeur=nul) et se déplacera jusqu'à la fin du fichier (EOF : End Of File).
C'est une des étapes les plus importantes dans la réalisation de la supervision. Chaque ligne parcourue est ajoutée dans une variable temporaire « **data** ». Si la variable est vide (ligne vide), on passe à la ligne suivante. Si la variable contient des données, un test sera effectué pour rechercher les mots clés. Dans l'exemple ci-dessous, la fonction va rechercher dans la variable **data** le mot clé « **GROUPE_INCIDENT:** » en respectant la casse. Une seconde contrainte impose que ce mot clé doit obligatoirement en début de ligne (le plus à gauche ➔**Left**) pour être pris en compte.

Exemple : **GROUPE_INCIDENT: ATS_SESD_FR_DIS_AMCS**

Le codage sera:

if(**left**(**data**,len("**GROUPE_INCIDENT:**"))="**GROUPE_INCIDENT:**") then

Ce principe est appliqué à l'ensemble du fichier de configuration. Lorsqu'un mot clé est retrouvé, les données seront extraites en découpant la variable temporaire (**data**) en partant de la droite. Ce découpage consiste à déduire à partir de la droite la taille du mot clé de la taille de la variable.

Group_incident=**right**(**data**,len(data)- len("**GROUPE_INCIDENT:**")

Note : Il ne faut pas confondre :

Group_incident ➔ **la variable**
GROUPE_INCIDENT: ➔ **la donnée**

Une autre solution consisterait à remplacer (**replace**) chaque mot clé dans la variable temporaire par «**vide**», comme dans l'exemple suivant.

Group_incident=**replace**(**data**,"**GROUPE_INCIDENT:**", **""**)

Cette dernière solution n'a pas été retenue, mais les deux solutions sont équivalentes. Le choix qui a été fait est purement arbitraire.
La variable **Group_incident** dans notre exemple contient «**ATS_SESD_FR_DIS_AMCS** » , avec ou sans espace en début et fin de chaîne. Afin que cette donnée soit exploitée, les espaces non désirés seront éliminés. La commande ci-dessous permet de supprimer les espaces dans le contenu de la variable group_incident.

Group_incident=**replace**(**Group_incident**," ","")

La lecture automatique de la configuration a permis d'ajouter des nouvelles fonctionnalités dans la supervision. Toute la configuration est ainsi déportée dans les fichiers de configuration. Les codes source ont été développés autour des fichiers de ces différents fichiers.
Il existe d'autres solutions, comme le passage des paramètres de configuration en argument à chaque programme de la supervision. Mais cette dernière n'a pas été retenue. Le nombre de paramètres serait trop nombreux et risquerait d'être une source d'erreurs.

IV.1.4.3 Création des tickets de suivi des incidents

Lorsqu'un incident est détecté dans la plage de service, un courriel sera envoyé à la boite aux lettres destinée à la gestion automatique des tickets d'incidents. L'application de gestion des incidents contient un connecteur de courriels. Le connecteur de courriel est une interface qui relie une application à un système de messagerie pour faciliter la lecture des messages ou courriel. C'est le principe de la lecture automatique de document (LAD). Le contenu du courriel sera analysé pour en extraire les informations. L'éditeur de l'application Cornerstone, la société HP, a fourni la trame des mots clés. Ces mots clés sont constitués de balises (ou délimiteurs) et seront placés le corps du message. Quelques exemples de balises sont fournis ci-dessous.

- Le type de ticket à créer est « **incident** » et doit être encadré par les balises ci-dessous.
  - **<TICKETTYPE><![CDATA[incident]]></TICKETTYPE>**

- Le groupe d'affectation du ticket est encadré par les balises ci-dessous. Le groupe d'affectation est **ATS_SESD_FR_DIS_AMCS**.
  - **<GROUP><![CDATA[ATS_SESD_FR_DIS_AMCS]]></GROUP>**

- Le mot clé «**CreateTicket** », encadré par les balises, indique la fin du message et que le ticket peut être créé.
  - **</CreateTicket>**

La supervision ne gère pas les tickets dans la base. Son rôle est d'envoyer le mail en respectant le bon format et les informations indispensables pour la création du ticket. La figure 37 est un ticket de suivi créé par la supervision active directory.

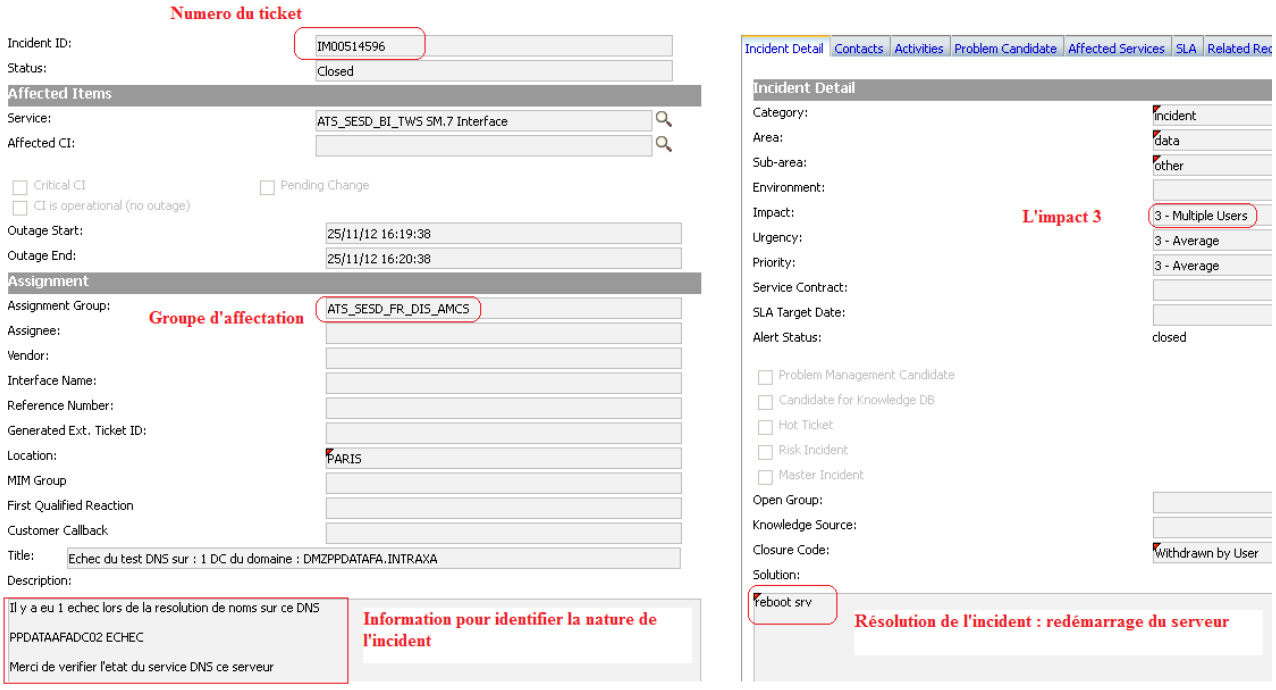


Figure 37 : Exemple de ticket de suivi créé par la supervision

La supervision a besoin de l'ordonnanceur pour planifier les contrôles. Les travaux et flux de travaux sont des éléments incontournables dans le projet.

IV.2 Création des travaux ou Jobs dans TWS

La création des travaux (jobs en anglais) dans TWS est une étape importante dans la gestion de la supervision. Le but de ce chapitre n'est pas de mettre en place un ordonnanceur, mais d'utiliser l'ordonnanceur existant. La supervision est compatible avec tous ordonnanceurs ou gestionnaire de tache Windows. Toutes les étapes de la création des travaux ne seront pas représentées. Seules les étapes importantes seront reprises.

IV.2.1 Les informations élémentaires

La création des travaux dans TWS nécessite d'avoir des informations élémentaires propre à ATS. Les tableaux 15 et 16 représentent une partie de ces informations nécessaire à la réalisation du projet. Le tableau 15 fournit la liste des périmètres clients et les codes associés.

Périmètre	Code Périmètre
Autres Clients	A
France	F
Med Région	R

Tableau 15 : Correspondance des périmètres clients chez ATS

Le tableau 16 est un extrait des codes des environnements de travail. D'autres environnements existent mais n'ont pas de relation avec le projet.

Environnement	Nom d'Environnement	Code Environnement
Production	Prod	P
Pré-production	Pprd	T
Intégration Applicative	Intg	I
Développement	Devl	D

Tableau 16 : Correspondance des environnements de travail

IV.2.2 Création des flux de travaux ou jobstream

Les travaux sont gérés par E-Gen, une application installée sur le mainframe. Le client E-gen permet de l'administrer depuis des ordinateurs Windows. Un mot compte et un mot de passe seront requis pour s'y connecter. Il s'agit du compte RACF[32], un programme de sécurité qui gère les contrôles d'accès.

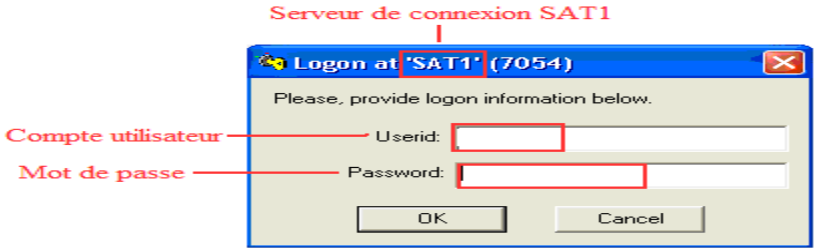


Figure 38 : Connexion à E-Gen

[32] RACF : Ressource Access Control Facility, ou gestion des contrôles d'accès aux ressources en français

Les créations de travaux sont toujours faites dans le « **stage EDIT**» ou phase de modification. Les travaux seront ensuite montés dans le « **stage PPRD**» (pre-production ou qualification). Et enfin ils seront générés l'environnement **PROD** (ou production).Les travaux déjà en production devront d'abord être rapatriés en **HOTFix** (maintenance à chaud) pour être modifiés. La figure 39 présente les « stages » disponibles.

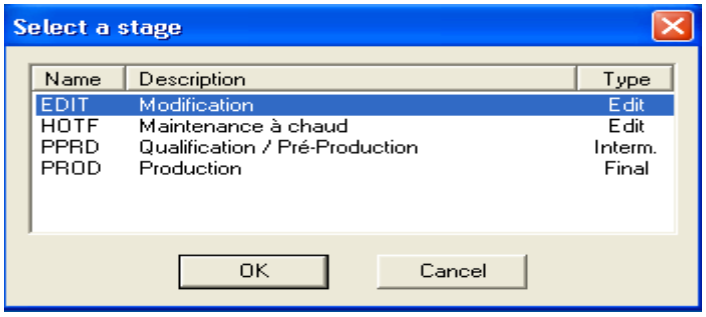


Figure 39 : Etapes de maintenance des travaux

Les flux travaux seront créés dans le stage EDIT dans TWS (OPC[33]).

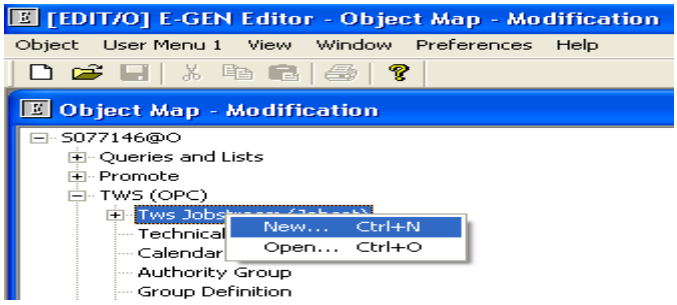


Figure 40 : Création d'un nouvel objet dans TWS

Les flux travaux à créer seront du type cyclique ou « **jobstream Acyclique** ». Le type « Acyclique » détermine la périodicité des travaux et est représenté par le point (1) sur la figure 41. Ils seront exécutés toutes les 30 minutes.

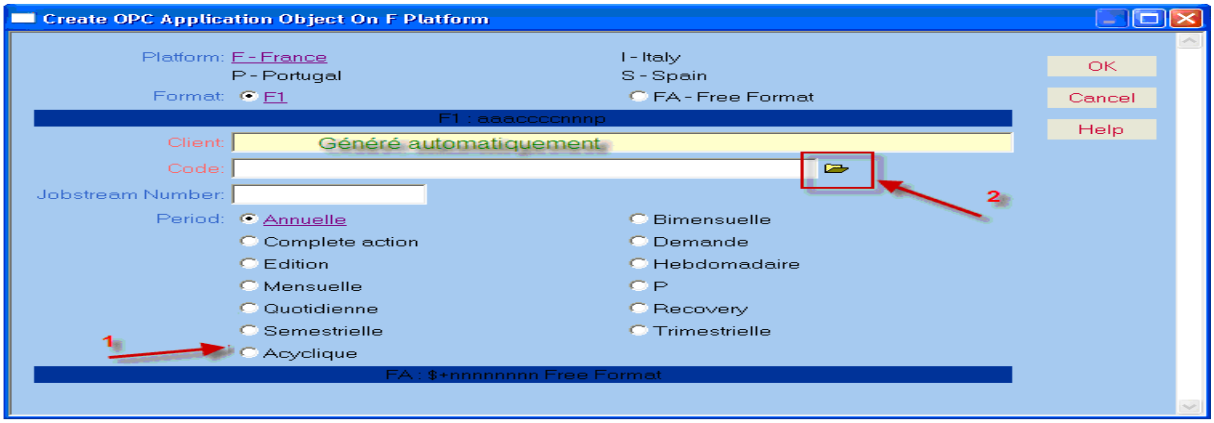


Figure 41 : Choix de la périodicité

[33] OPC : Operations Planning and Control (planification et contrôle des opérations en français)

Lorsque la périodicité est sélectionnée, le code applicatif sur lequel s'exécuteront les travaux devra être validé en sélectionnant le dossier « **code** » (2), figure 41.
Dans « **Open Name** » il faut saisir **F+TSWA** puis sélectionner ce code applicatif. Le code applicatif « **F+TSWA** » est le code applicatif générique pour la « France » en mode « création». Voir tableau 15 et 16.

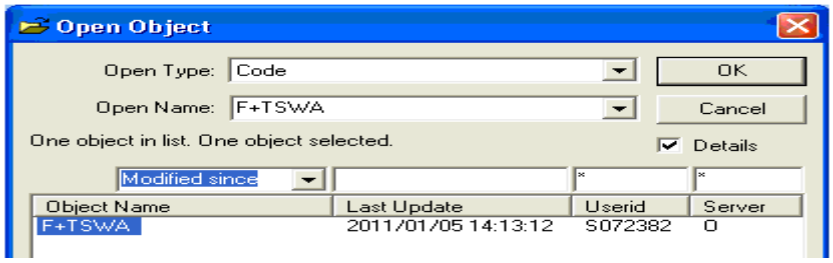


Figure 42 : Sélection du code applicatif dans E-Gen

Lorsque le code applicatif est sélectionné, il faut choisir le client pour lequel les travaux seront exécutés. Il s'agit des clients d'ATS. Les clients ont été créés par les administrateurs de l'ordonnanceur. Ce sera un flux de travaux mutualisé, c'est-à-dire partagé par plusieurs clients. Le client Axa France (AFA) possède le plus de serveur, il sera sélectionné par défaut.

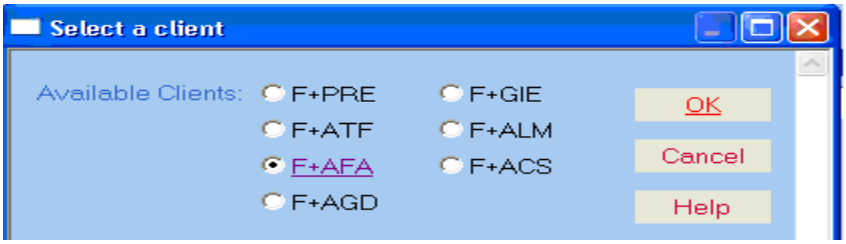


Figure 43 : Choix du client

L'étape suivante consiste à numéroter le flux de travaux. Un fichier de suivi référençant tous les travaux est disponible. C'est le fichier « **LIST_WKLD_JOBSETS.xls** ». Il faut choisir un numéro disponible dans ce fichier pour créer le flux de travaux.

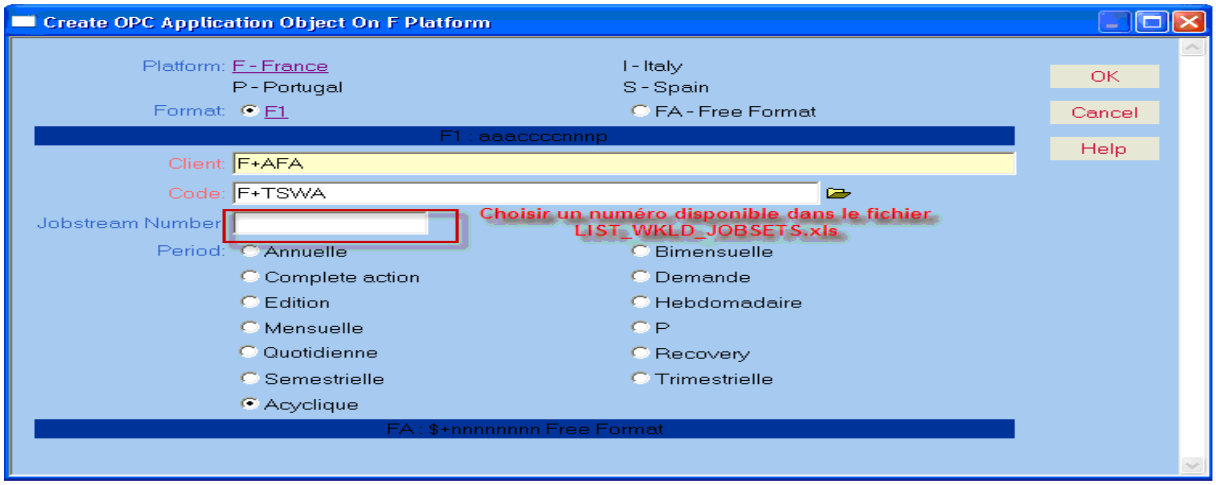


Figure 44 : Création d'un flux de travaux ou jobstream

Le calendrier définit les jours d'exécution des travaux. La planification est disponible en cliquant sur le dossier (1) dans le champ « **calendar**» ou calendrier en français.

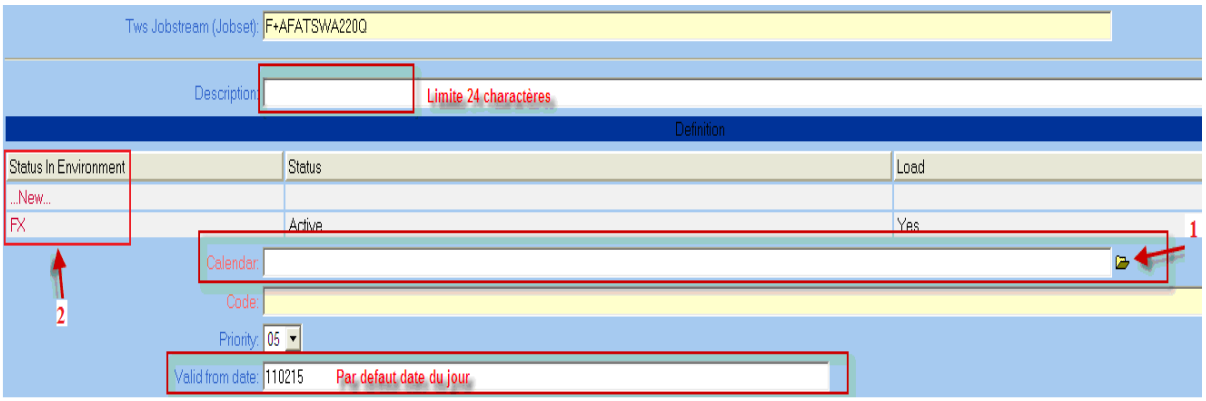


Figure 45 : Finalisation du Jobstream

Le détail du calendrier est fourni en annexe 1. Il fournit les informations nécessaires pour la compréhension de ces codes.

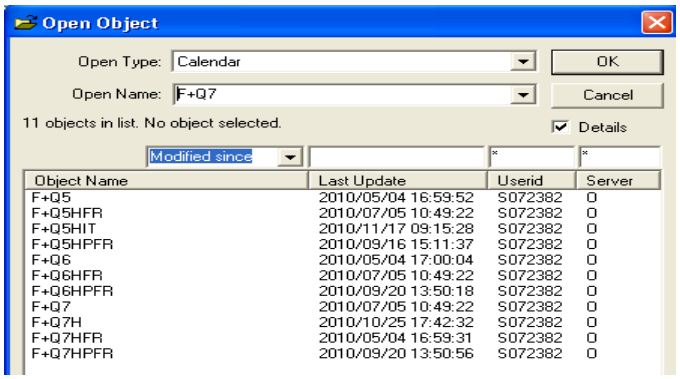


Figure 46 : Les références du calendrier dans E-Gen

Le champ « **Status in Environnement** » (figure 45, point 2) permet de spécifier le statut du jobstream par environnement. Dans le cas présent le job sera actif sur tous les environnements (**FX**). Car le jobstream devra passer par plusieurs environnements avant d'arriver en production. La figure 47 indique les environnements possibles pour un jobstream.

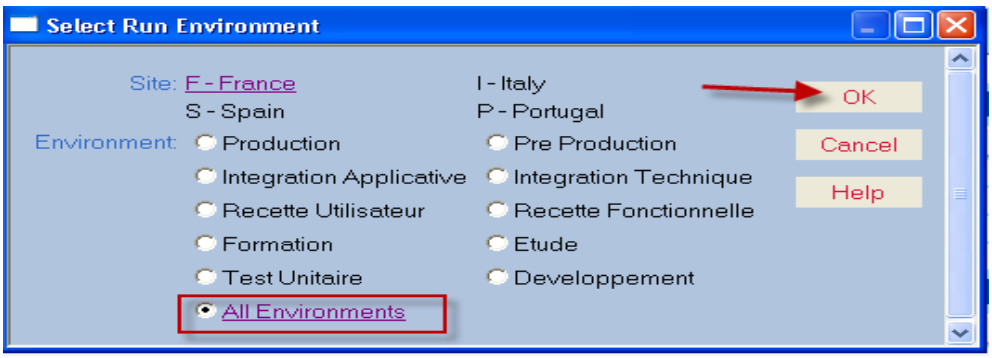


Figure 47 : Choix des environnements

Il est possible de choisir différents mode de planification : quotidien, hebdomadaire, mensuel, etc. Dans le cadre du projet, la supervision sera en production du lundi au samedi et planifiée toutes les 30 minutes. Le calendrier sera du type Q6 (6 jours), comme indiqué en annexe 1.

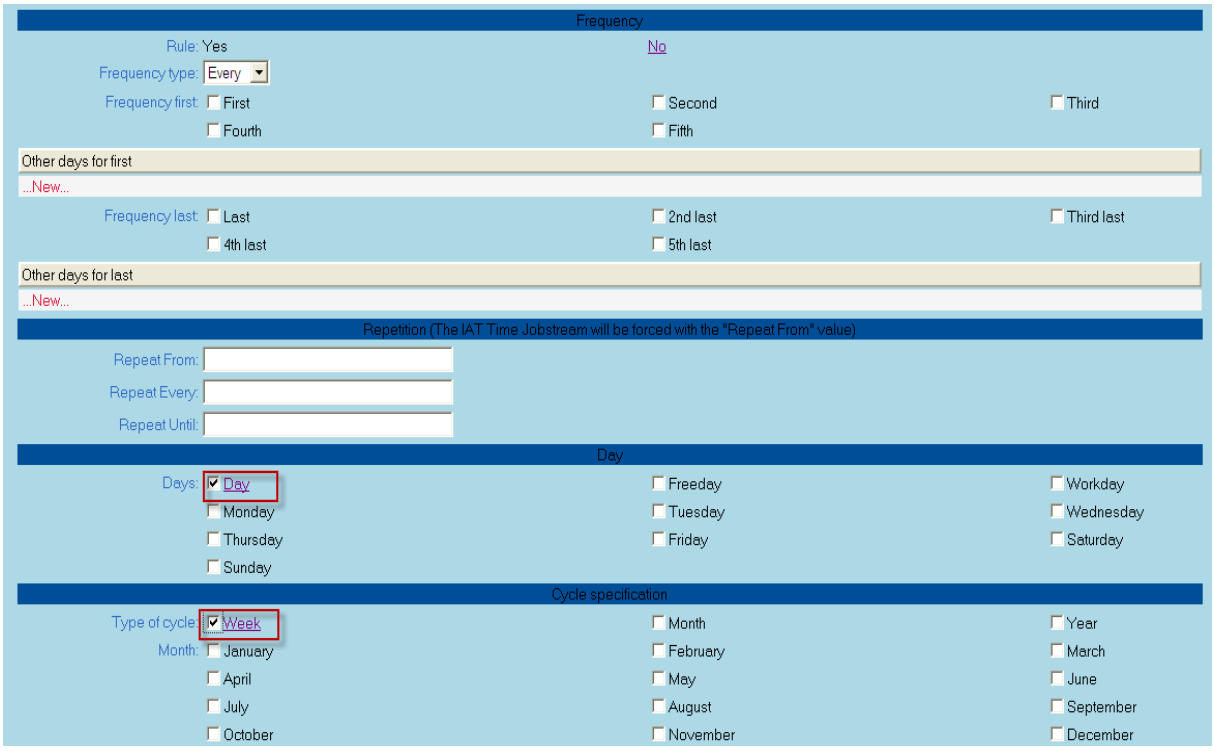


Figure 48 : Planification des flux de travaux ou jobstream

IV.2.2.1 Création des travaux ou jobs

Les travaux définissent les actions à réaliser. Ils seront exécutés par l'ordonnanceur selon la planification qui a été faite précédemment. Dans le champ « **Operations** » de la figure 49, deux éléments sont déjà présents. Il s'agit des jobs **009-GEG** et **255-END**, job de début et de fin de Jobstream. Ils sont créés automatiquement par le système. Les travaux viendront s'intercaler entre ces deux jobs.

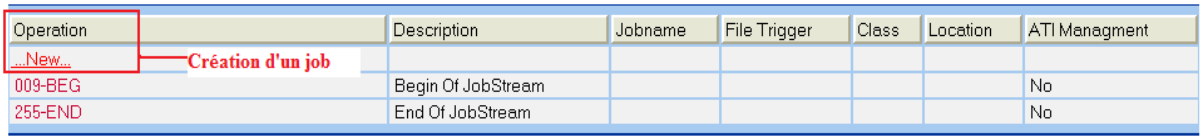


Figure 49 : Création d'un nouveau Job

Les travaux à créer sont du type « **script** ». Ils seront utilisés pour exécuter le lanceur. Le type de traitement sera « **Vision Supervision Surveillance**». La première opération dans le champ « **opération number** » ou numéro d'opération en français débutera à 40. Les numéros d'opérations devront entre compris entre 40 et 250.

Les autres numéros sont réservés pour les travaux de maintenances. Le « **job number** » ou numéro de travaux commence à 005 et sera incrémenté de 5 en 5. La figure 50 illustre les opérations effectuées.

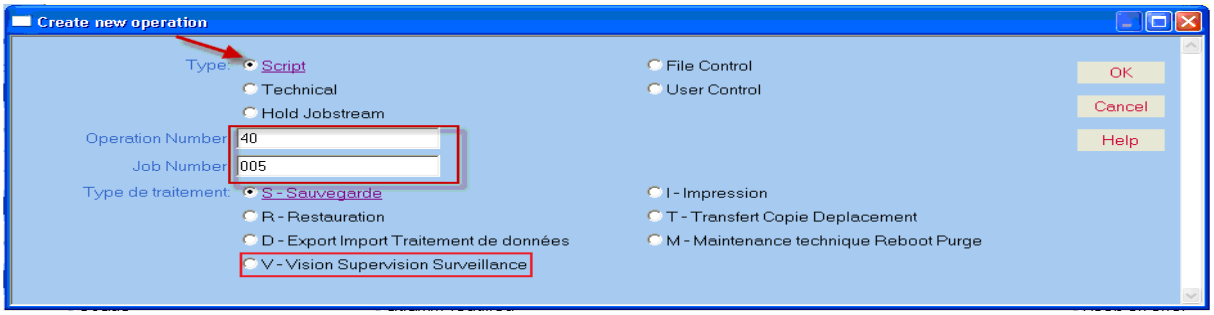


Figure 50 : Définition d'un job

La mise en production de la supervision nécessite de créer autant de jobs que de domaines à superviser. Pour faciliter la gestion de la supervision, deux jobsstream seront créés. Un josbstream pour les domaines de production et un autre pour les autres environnements.

- **La notion de location**

La localisation ou « **location** » en anglais, est un objet permet de décrire, le serveur, le type d'utilisateur, le mot de passe de l'utilisateur exécutant les travaux, etc. L'objet « location » contient également les versions du système d'exploitation des serveurs. Cette information est utilisée pour contrôler la cohérence des serveurs : Linux, Windows, etc. Il est utile pour gérer les accès aux scripts.

Remarque : Une location peut être utilisée par plusieurs serveurs mais uniquement du même domaine. Un compte a été créé par ATS dédié à l'exécution des travaux dans chaque domaine. Il a le privilège de se connecter en tant que gestionnaire de scripts et est administrateur local tous les serveurs.

Important : La location correspond au serveur superviseur. Il est sous la forme F+TSWA-XXX, ou XXX est un incrémental numérique. Le flux de travaux sera composé de plusieurs « locations ».

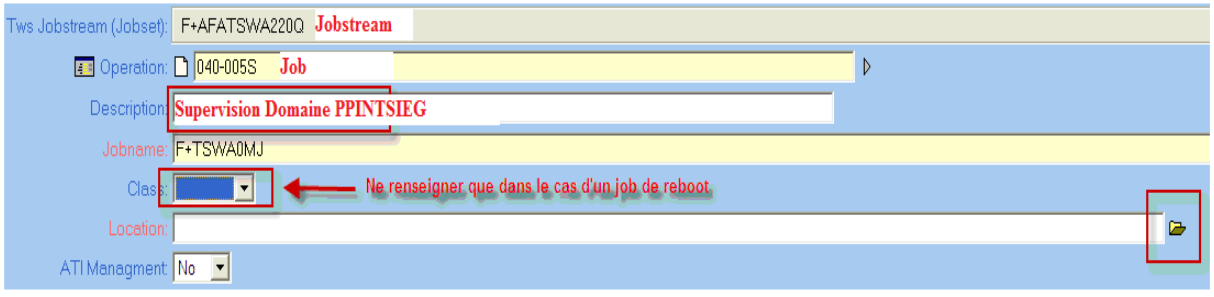


Figure 51 : un job dans un jobstream

En sélectionnant le dossier location, la liste de toutes les locations apparaîtra. Il suffira de juste de choisir celle qui correspond. Si la location ne convient pas, les travaux ne seront pas exécutés, car le compte présent dans la location n'aura pas les privilèges nécessaires pour exécuter les travaux.

De nombreux paramètres sont disponibles dans pour les jobs. Une brève description est fournie ci-dessous en rapport avec la figure 52.

Inactive environnement : spécifie l'environnement dans lequel le job ne tournera pas.
Recovery on Abord : permet de lancer un autre job en cas d'échec.
Parameter : possibilité de spécifier des paramètres pour le lancement du script.
Return Code : code retour maximal autorisé et sera en « erreur» s'il est supérieur.
Must Sart Time : déclenche une action si le job n'est pas lancé à l'heure définie.
Must End Time : déclenche une action si le job n'est pas terminé à l'heure désirée.
Max Time Duration : déclenche une action si le job dépasse une certaine durée d'exécution.

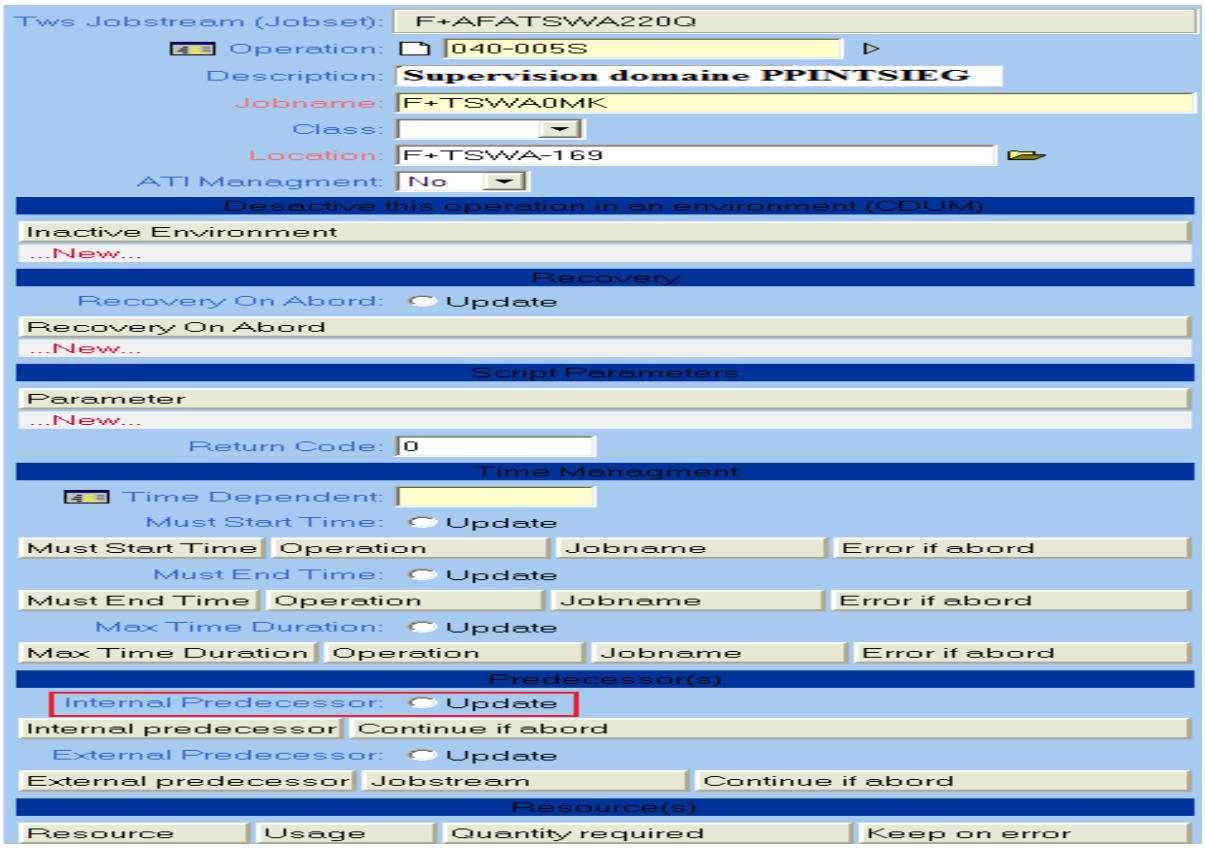


Figure 52 : Récapitulatif du job

Un job doit toujours être relié à un job de début et à un job de fin de manière contiguë ou non. L' « **Internal predecessor** » ou prédécesseur interne permet de spécifier le prédécesseur du job à l'intérieur du Jobstream. Dans notre cas le prédécesseur sera le job 009-BEG. Pour modifier le prédécesseur, il suffit de cliquer sur « update » au niveau de « **internal predecessor** ». La figure 53 illustre les options possibles pour les prédécesseurs.

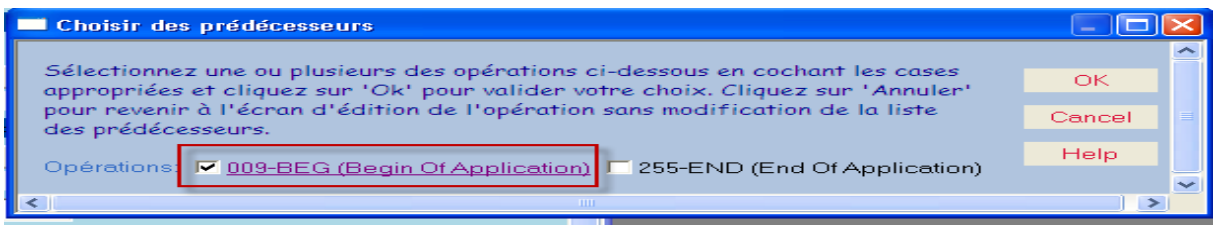


Figure 53 : Les prédécesseurs du job courant

Le prédécesseur de l'opération « **40** » a été défini, il reste à définir le prédécesseur de l'opération de fin 255. Le job de fin 255 sera relié à son tour au job numéro 40. Cette opération est réalisable dans la section « **external predecessor** » ou prédécesseur externe, figure 52.

IV.2.3 Ajout des jobstream au plan

Le jobstream est construit mais n'est pas encore monté au plan de production. Il a été défini en mode EDIT, il devra d'abord être monté (ou généré) en pre-prod et ensuite en production. Cette opération est possible à l'aide du bouton « **generate** » ou générer en français dans chaque environnement, comme indiqué dans la figure 54.

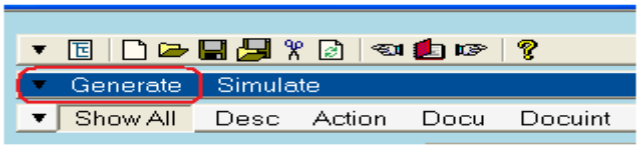


Figure 54 : Génération du job dans les environnements

Lorsque le job ou le jobstream est arrivé en production, il est prêt pour la montée au plan. La figure 55 montre les options pour la mise au plan. Cette étape permet d'ajouter le jobstream dans le plan courant à l'aide du bouton : « **add a jobstream to current plan** ». Les informations concernant le plan courant sont décrites au paragraphe II.4.1.3.

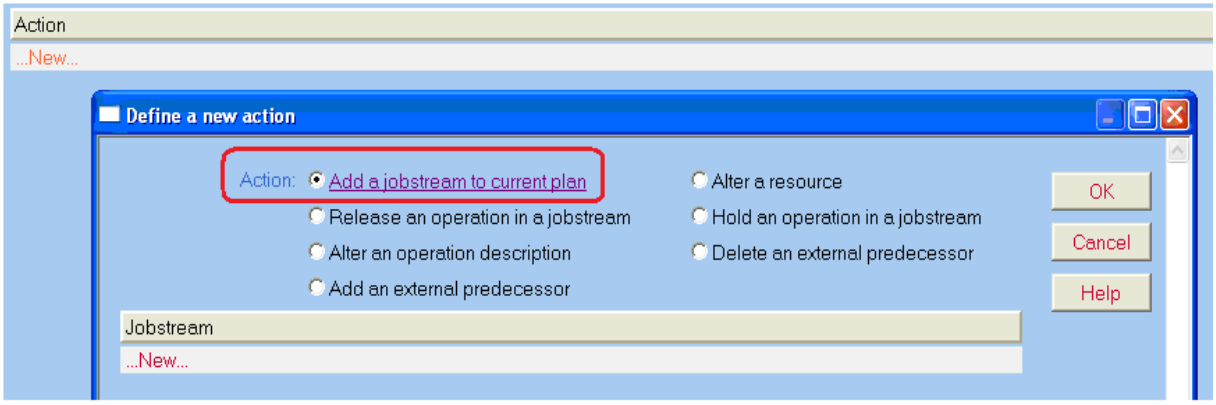


Figure 55 : Ajout au plan courant

Les informations essentielles concernant la création du jobstream ont été fournies. La programmation de l'exécution de la supervision est terminée. Le jobstream s'exécutera tous les jobs associés. Chaque job correspond à la supervision de chaque domaine d'ATS. Les environnements hors production permettent des jeux de tests sur la l'ordonnanceur et la supervision.

V Le bilan global

Le projet est terminé, il est temps de faire le bilan global. Les exigences d'Axa Technology Services (ATS) ont été respectées en utilisant des outils dont les sources sont fiables. La supervision a permis d'éviter de nombreux incidents visibles par les utilisateurs. Le projet a été réalisé sans budget, ce qui a permis de réduite les dépenses liées aux systèmes d'information d'ATS. C'est donc un bilan très positif pour le projet.

V.1 Le défi technique

Le projet a été un vrai défi technique. Il fallait répondre aux exigences d'ATS et proposer une solution technique fiable et facile d'utilisation. L'utilisation des outils de bases de Microsoft Windows pour réaliser la supervision a été un vrai défi technique. Les outils de supervision étaient encore jusqu'ici réservés des éditeurs avec des armés d'experts.
La conception de la supervision a été réalisée selon un principe novateur, en proposant une supervision sans installation (portable). Les codes sources ont été créés pour être génériques et utilisables dans tous les domaines active directory. La modélisation a permis de gagner du temps sans s'éloigner du résultat attendu.
L'intégration de l'ordonnanceur TWS dans la supervision a permis centraliser la gestion de la supervision. Ainsi TWS est utilisée comme une console d'administration pour l'ensemble des supervisions. TWS embarque des fonctionnalités de création automatiques de tickets d'incident dans le logiciel de gestion des incidents d'ATS. Il permet ainsi de contrôler la supervision en cas de disfonctionnement de son exécution.
En proposant la supervision Active Directory à ATS, j'ai montré qu'il était possible de réaliser des outils peu coûteux répondant à des problématiques assez complexes.

V.2 L'évaluation de la supervision

Les tests de non régression ont été effectués tout au long du projet. Grâces aux tests, des améliorations ont ainsi pu être apportées afin de gagner en fiabilité. Les alertes remontées par la supervision se sont révélées exactes.
La supervision active directory a permis à de nombreuses reprises d'alerter les équipes techniques avant même que les utilisateurs ne s'aperçoivent de l'anomalie. Elle occupe une place de plus en plus importante dans la gestion de l'active directory. Toutes les alertes reçues sont prises en compte, car la supervision a fait ses preuves au cours de la période d'évaluation.
La supervision ne fait qu'alerter. La réactivité des équipes exploitantes est donc un facteur déterminant lors de la détection d'un incident. Plus vite l'incident sera résolu et moins les conséquences seront importantes.
Des améliorations devront être apportées pour gagner en performance, mais la supervision est toutefois très fiable. La supervision est évolutive. De nouvelles fonctionnalités pourront être ajoutées pour prendre en comptes les évolutions de l'active directory.
Il est possible de tester réplications et s'assurer qu'elles sont opérationnelles sur l'ensemble des contrôleurs de domaines. Cette évolution n'est toute fois pas indispensable. La vérification des réplications fait parti des vérifications quotidiennes des administrateurs et ingénieurs systèmes.

V.3 Le bilan du projet

En proposant une solution de supervision à un coût réduit, avec uniquement le budget de fonctionnement, j'ai pu ainsi répondre aux exigences du responsable du service.
Les incidents ont été mis sous surveillance grâce à la supervision. Ils sont souvent détectés et résolus avant leurs détections par les utilisateurs. La réactivité de l'équipe exploitante a joué un très grand rôle.
Les incidents sur l'infrastructure active directory sont moins visibles et voir quasiment nulles pour les utilisateurs. La confiance des utilisateurs est revenue progressivement, ainsi que celle de la direction d'AXA.
Le projet a été couronné d'un grand succès. Il a permis de mettre en avant les initiatives locales entreprises par le service, géré par Olivier M. Ce projet a montré mes capacités à mener à bien un projet et à y apporter une solution.
La réussite du projet a été possible grâce au responsable du service qui m'a fait confiance en me laissant carte blanche dans le choix de la solution.

V.4 Le bilan personnel

La réalisation de ce projet chez un grand groupe comme ATS a été pour moi une expérience très enrichissante. La diversité de l'environnement technique et la taille de l'infrastructure active directory m'ont permis d'avoir un support de travail consistant pour mener à bien ce projet.
J'ai su montrer mon savoir faire et valoriser mes compétences. Mon travail a été reconnu aussi bien par le responsable du service que par l'ensemble des acteurs d'ATS. La réussite du projet est bien plus qu'une récompense, car grâce à cette expérience enrichissante chez ATS, je réalise mon projet de mémoire au CNAM.
C'est aussi l'aboutissement de plusieurs années d'investissement personnel et un bilan professionnel très positif.
J'ai ainsi pu contribuer à des projets de grande envergure au niveau du groupe AXA. J'ai été reconnu pour ma capacité à proposer des solutions d'industrialisation et à gérer des environnements techniques très variés. ATS est une plateforme technique riche et variée qui permet à des ingénieurs d'exprimer leur talent.

VI Conclusion générale

AXA Technology Service ou ATS est une filiale du groupe AXA. La diversité de ses activités classe ATS dans la catégorie des fournisseurs d'accès.
De nombreux incidents sur l'infrastructure active directory d'ATS entre 2011 et 2012, non détectés par l'outil de supervision NSM3.1, ont beaucoup affectés les clients et utilisateurs d'AXA. Le manque de confiance des utilisateurs et la direction générale dans le système d'information d'ATS nous ont conduits à revoir la supervision existante. Bien que le budget réservé au système d'information à considérablement diminué, la Direction du Système d'Information (DSI) doit répondre aux exigences des utilisateurs et de la direction générale. Ces exigences ont beaucoup évolués durant ces dernières années.
L'arrivée de nouveaux moyens de communication fait du système d'information un atout capital pour l'entreprise. L'active directory est un annuaire distribué d'entreprise qui permet une gestion centralisée des accès. Il constitue le cœur de l'infrastructure du système d'information. De nombreuses applications de l'entreprise nécessitent une connexion à cet annuaire pour fonctionner efficacement. Des incidents sur l'active directory peuvent perturber fortement les activités de l'entreprise.
La DSI doit de plus en plus composer avec les restrictions budgétaires tout en répondant aux exigences des utilisateurs et des clients d'ATS. Des outils obsolètes continuent d'être utilisés tant qu'ils couvrent une part importante des besoins de l'entreprise. Ainsi la supervision active directory est très souvent reléguée au second plan. Les coûts pour la mise à niveau d'une supervision représentent un budget considérable. Les besoins immédiats et souvent justifiés sont prioritaires. La gestion des risques, ou devrais-je dire « la gestion des priorités », est souvent centrée sur le besoin des utilisateurs. Les risques liés à l'infrastructure du système d'information ne doivent pas être sous estimés. Les pertes financières liées aux incidents sur le système d'information sont difficilement chiffrables. Mais les économies réalisées par les restrictions budgétaires du système d'information ne couvriront sans doute pas les pertes qu'elles ont engendrées.
La supervision active directory est la surveillance de l'ensemble des serveurs qui héberge l'annuaire distribué. Elle utilise plusieurs moyens pour alerter lors de la détection d'un incident. Des solutions existent sur le marché, mais nécessitent une infrastructure de supervision dédiée.
Afin de répondre aux exigences d'ATS, j'ai développé une supervision portable, c'est-à-dire sans installation. Elle ne nécessite pas d'architecture de supervision dédiée, réduisant considérablement les coûts d'implémentation et de maintenance. Elle utilise majoritairement les outils natifs de Windows, ce qui la rend compatible avec toutes les versions du système d'exploitation de l'éditeur Microsoft. Elle journalise tous les contrôles et alerte par courriel en cas d'incidents sur l'active directory. Le courriel est formaté afin de générer un ticket dans la base de suivi des incidents d'ATS.
La supervision propose de nombreuses options, telle que la plage de maintenance automatique, la prise en charge des fuseaux horaires, etc. Elle a été conçue en prenant en compte les exigences d'ATS d'une part et les besoins des ingénieurs système d'autre part. L'intégration de l'ordonnanceur dans le fonctionnement de la supervision permet une gestion centralisée.
La supervision active directory a su trouver sa place en alertant les équipes lors de la détection d'incidents. Les équipes d'exploitation sont dès lors plus réactives pour résoudre l'incident. La confiance des utilisateurs est revenue peu à peu, et les remontées d'incidents sur l'infrastructure active directory par les utilisateurs sont quasiment nulles.

En proposant une solution de supervision efficace j'ai su montrer mon savoir faire. J'ai utilisé les outils conçus pour les taches d'administration courantes, pour automatiser l'ensemble des contrôles. Cette expérience très positive de la supervision au sein d'ATS m'a permis de travailler sur d'autres projets de grande envergure. Ma valeur ajoutée au sein d'ATS est ma capacité à proposer des solutions d'automatisation et d'industrialisation. ATS possède un parc de plus de 3000 serveurs Windows pour lesquels des taches de maintenance sont nécessaires. L'automatisation de ces maintenances permet de garantir un traitement standardisé.
En attendant la migration de la supervision NSM3.1 vers la nouvelle version NSM r11 de Computer Associates (CA), des évolutions sont prévues par les équipes d'ATS afin d'implémenter de nouvelles fonctionnalités. Une étude doit aussi être faite pour une migration vers « **powershell** », le nouveau langage natif à toutes les nouvelles versions de Microsoft Windows (depuis windows 2008 serveur).

VII Abréviations et glossaire

AD	Active Directory
API	Application Programming Interfaces
ATS	Axa Technology Services
Attributs	un attribut est une propriété d'un objet, exemple : âge, couleur, etc.
CA	Computer Asscicates
CAB	Comité d'Approbation des Changements
Classes	au sens active directory, une classe d'objet est un regroupement d'attributs
CNAM	Conservatoire National des Arts et Metiers
CNAME	Canonical NAME (se prononce cénèïme)
CRIM	Compte Rendu des Incidents Majeurs
CSV	Comma-Separated Values
DAP	Directory Access protocol
Data Center	Centre de traitement des données
DB2	Data base 2, système de gestion de base de données développé par IBM
DC	Domain Controller
DES	Data Encryption Standard
DNS	Domain Name System
DOM	Département d'Outre-Mer
DOS	Disk Operating System
DSI	Direction des Systèmes d'Information
DSM	Distributed State Machine
EOF	End Of File
Fôret	La fôret au sens active directory est la hiérarchisation des domaines
FSMO	Flexible Single Master Operations
GUID	Globally Unique Identifier
HP	Hewlett-Packard (Société multinationale américaine)
HSA	Hardware System Area
IBM	International Business Machines
IDST	Infrastructure, Déploiement, Support et Télédistribution
IHM	Interface Homme-Machine
IP	Internet Protocole
ISC	International Software Company
ISO	International Organization for Standardization
LAD	Lecture Automatique de Documents
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Secure
LPAR	Logical Partition
MO	Mega Octet
MOE	Maitrise d'oeuvre
MS-DOS	Microsoft-Disk operating system
NAS	Network Attach Storage
NetBIOS	Network Basic Input/Output System
NSM	Network and Systems Management
NTLM	(Windows) New Technology Lan Manager
OPC	Operations Planning and Control
Pare-feux	un est système de filtrage des paquets sur le réseau et de protection
PDC	Primary Domain Controller

Proxy	est un système qui sert d'intermédiaire pour accéder à des ressources
RACF	Ressource Access Control Facility
Ressources	Les ressources regroupent tous les services proposés par l'entreprise : Ex : fichiers, courriels, base de données, etc.
RID	Relative Identifier
SC	Service Control
Schéma	Contient les définitions de chaque classe d'objet pouvant être créée dans une forêt Active Directory
SGBD	Système de gestion de base de données
SID	Secure IDendifier
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSII	Société de Services Informatique et Ingénierie
SSL	Secure Sockets Layer
SSO	Single Sign-On
TGT	Ticket Grant Ticket
TMA	Tierce Maintenance Applicative
TWS	Tivoli Workload Scheduler (IBM)
VM	Virtual Machine
VBS	Visual basic script
WMI	Windows Management Instrumentation
Z/OS	zSeries/Operating System

VIII Médiagraphie

[1] CHARTIER E., préface RUFF A., Le système d'information du risque opérationnel : *Anticiper Alerter Evaluer*, Economica, 230p., 2008

[2] LEFEARD B., BOUQUET F., PICKAERT N., Industrialiser le test fonctionnel : *Pour maîtriser les risques métier et accroître l'efficacité du test*, Dunod, 292p., 2011

[3] Documentation de TWS 8.6, Guide d'utilisation et référence, IBM, 2009
Lien : http://publib.boulder.ibm.com/tividd/td/TWS/SC32-1274-02/fr_FR/PDF/SRF_mst.pdf

[4] Présentation de l'Active directory, Microsoft, 2005
Lien : http://technet.microsoft.com/fr-fr/library/cc781408(v=ws.10).aspx

[5] DNSCMD, les options d'utilisation, Microsoft,
Lien : http://technet.microsoft.com/fr-fr/library/cc772069(v=ws.10).aspx

[6] Prendre ou transférer des rôles FSMO, Microsoft, 2013
Lien : http://support.microsoft.com/kb/255504/fr

[7] NSM 3.1, Computer Associates, 2003
Lien : ftp://mf.cai.com/pub/downloads/UNI31/docs/README.HTML

[8] Identificateurs de sécurité (SID) connus, Microsoft, 2013
Lien: http://support.microsoft.com/kb/243330/fr

[9] Concept des protocoles d'authentification, Microsoft, Mise à jour 2013
Lien : http://technet.microsoft.com/fr-fr/library/cc757589(v=ws.10).aspx

[10] Introduction au langage Visual Basic Script, Developpez, Club des développeurs et IT Pro, Mise à jour 2002
Lien : http://tahe.developpez.com/web/vbscript/

Annexes

Annexe 1 : Le calendrier dans E-Gen, fourni par Axa Technology Services

Le calendrier permet planification des travaux dans l'ordonnanceur TWS.

Détail des différents calendriers	
Q5	5 jours ouvrés de la semaine : lundi à vendredi
Q6	6 jours ouvrés de la semaine : lundi à samedi
Q7	7 jours ouvrés de la semaine : lundi à dimanche

Q5HFR, Q6HFR, Q7HFR comme Q5, Q6, Q7 + jours féries suivants :	Q5HPFR, Q6HPFR, Q7HPFR comme Q5, Q6, Q7+ jours féries suivants :
01/01/10 jour de l'an	01/01/10 jour de l'an
05/04/10 pâques	05/04/10 pâques
01/05/10 fête du travail	01/05/10 fête du travail
08/05/10 armistice	08/05/10 armistice
13/05/10 ascension	13/05/10 ascension
24/05/10 pentecôte	24/05/10 pentecôte
14/07/10 fête nationale	14/07/10 fête nationale
15/08/10 assomption	15/08/10 assomption
01/11/10 toussaint	01/11/10 toussaint
11/11/10 armistice	11/11/10 armistice
25/12/10 noël	25/12/10 noël
31/12/10 réservé opérations de fin d'année	31/12/10 pont jour de l'an

Annexe 2 : Les options de la commande DNSCMD

Commande	Description
DNSCmd /clearcache	Efface le cache du serveur DNS.
DNSCmd /directorypartitioninfo	Affiche des informations sur une partition d'annuaire d'applications DNS.
DNSCmd /enumdirectorypartitions	Répertorie les partitions de répertoire d'applications DNS pour un serveur.
DNSCmd /enumrecords	Répertorie les enregistrements de ressources dans une zone.
DNSCmd /info	Obtient des informations sur le serveur.
DNSCmd /recordadd	Ajoute un enregistrement de ressource à une zone.
DNSCmd /recorddelete	Supprime un enregistrement de ressource à partir d'une zone.
DNSCmd /statistics	Interroge ou efface les données statistiques du serveur.
DNSCmd /zoneadd	Crée une nouvelle zone sur le serveur DNS.
DNSCmd /zonedelete	Supprime une zone à partir du serveur DNS.
DNSCmd /zoneexport	Écrit les enregistrements de ressources d'une zone dans un fichier texte.
DNSCmd /zoneinfo	Affiche les informations de zone.
DNSCmd /zoneprint	Affiche tous les enregistrements dans la zone.
DNSCmd /zonerefresh	Force une actualisation de la zone secondaire à partir de la zone principale.

Annexe 3 : La commande SC, native windows

DESCRIPTION :
SC est un utilitaire de ligne de commande utilisé pour communiquer avec le Gestionnaire de contrôle des services et les services.

UTILISATION :
sc <serveur> [**commande**] [nom service] <option1> <option2>...
L'option <serveur> se présente au format « **NomServeur** »
Pour obtenir de l'aide sur une commande, entrez : « sc [**commande**] »

Commandes :

Query	Interroge l'état d'un service ou énumère l'état de types de services.
Queryex	Interroge l'état étendu d'un service ou énumère l'état de types de services.
start	Démarre un service.
pause	Envoie une demande de contrôle PAUSE à un service.
Interrogate	Envoie une demande de contrôle INTERROGATE à un service.
Continue	Envoie une demande de contrôle CONTINUE à un service.
stop	Envoie une demande STOP à un service.
config	Modifie la configuration d'un service (persistant).
Description	Modifie la description d'un service.
failure	Modifie les actions entreprises par un service en cas d'échec.
Failureflag	Modifie l'indicateur des actions d'échec d'un service.
sidtype	Modifie le type de SID d'un service.
privs	Modifie les privilèges nécessaires d'un service.
qc	Interroge les informations de configuration d'un service.
Qdescription	Interroge la description d'un service.
Qfailure	Interroge les actions entreprises par un service en cas d'échec.
Qfailureflag	Interroge l'indicateur des actions d'échec d'un service.
Qsidtype	Interroge le type de SID d'un service.
qprivs	Interroge les privilèges nécessaires d'un service.
delete	Supprime un service (du Registre).
create	Crée un service (en l'ajoutant au Registre).
control	Envoie un contrôle à un service.
Sdshow	Affiche le descripteur de sécurité d'un service.
sdset	Définit le descripteur de sécurité d'un service.
Showsid	Affiche la chaîne du SID de service correspondant à un nom arbitraire.
GetDisplayName	Récupère le nom affiché d'un service.
GetKeyName	Récupère le nom de clé d'un service.
EnumDepend	Énumère les dépendances d'un service.

Annexe 4 : Fichier de configuration config_ldap.ini

DOMAINE: Pour le nommage des fichiers dans la cartographie. Ex ; AFA.AXAPR_DCC
CHK_DOMAINE: Nom NETBIOS du domaine, ex : AXAPR
USER: Premier compte pour les tests d'authentification (compte1)
PASS_WORD: Identifiant numérique correspondant au mot de passe du compte1
USER: Second compte pour les tests d'authentification (compte2)
PASS_WORD: Identifiant numérique correspondant au mot de passe du compte2

TIME_START: Début plage de service et fin plage de maintenance
TIME_END: Fin plage de service et début de plage de maintenance
MAIL_BASE: Adresse du courriel pour la création du ticket de suivi des incidents.
GROUPE_INCIDENT: Groupe d'assignation des tickets de suivi des incidents
MAILTO: Liste des destinataires des courriels d'alertes, séparés par un point virgule « ; »
SMTP: Adresse IP du serveur SMTP de l'entreprise (ou serveur de relais de messagerie)

Copier/coller les 2 lignes suivantes autant de fois que de contrôleurs de domaines à superviser en respectant l'ordre **SERVER_NAME:** puis **IP_SERVER:**
SERVER_NAME: Nom du contrôleur de domaine
IP_SERVER: IP du contrôleur de domaine

Pour la gestion des fuseaux horaires
SERVER_NAME: Nom du contrôleur de domaine
EXECEP_TIME_STRT: Début de la plage de service spécifique, ex : 13:00:00
EXECEP_TIME_STP: Fin de la plage de service spécifique, ex : 23:00:00
IP_SERVER: IP du contrôleur de domaine

Section pour les tests DNS et vérification des enregistrements DNS

NS_NBR_SERVEUR: Cette option n'est pas utilisée. Elle correspond au nombre de contrôleurs de domaine superviseurs. (Pour la supervision des enregistrements DNS)

NS_CLIENT_NAME: Le nom du client propriétaire de l'environnement de travail
NS_EXCLUSION: Cette option n'est pas utilisée. Elle servira pour l'exclure
NS_DOMAINE: Nom de domaine pour les tests DNS : ex axa-tech.com

NS_SERVEUR_NAME: Nom du serveur superviseur des enregistrements DNS
NS_SERVEUR_IP: Adresse IP du serveur superviseur des enregistrements DNS

EX_NS_SERVER_NAME: Contrôleurs de domaine à exclure de la supervision DNS

Supervision des enregistrements DNS, à copier /coller autant de fois que nécessaire

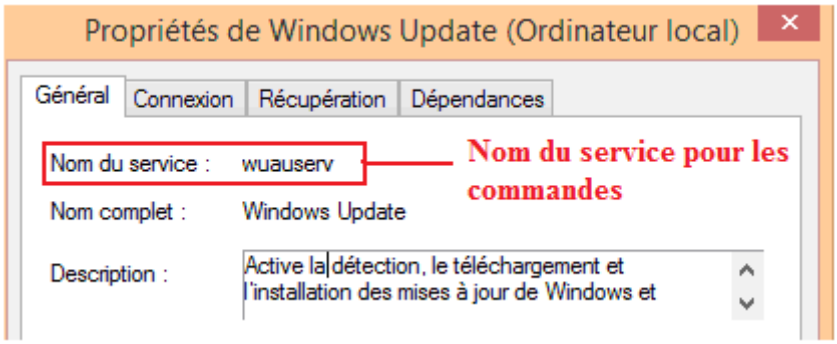
NS_CONTROLE_N: Nom de l'enregistrement à superviser
NS_CONTROLE_I: Adresse IP de l'enregistrement à superviser

Supervision des enregistrements DNS du type « alias »
NS_CONTROLE_N: Nom de l'enregistrement à superviser
NS_CONTROLE_A: Nom de l'alias à superviser
NS_CONTROLE_I: Adresse IP de l'enregistrement à superviser

Annexe 5 : un extrait du fichier des services : services.ini

Le nom complet du service peut différer d'une version à l'autre de Windows. Mais le nom du service sera le même pour des raisons de compatibilités.

#Nom du service ➔ Nom complet du service, il est à titre informatif
SERVICE_NAME: ➔ Nom du service
SERVICE_ID: ➔ ID du service pour la mise en forme dans la cartographie



Exemples :
#Net Logon
SERVICE_NAME: Netlogon
SERVICE_ID:0

#Kerberos Key Distribution Center
SERVICE_NAME: kdc
SERVICE_ID:0

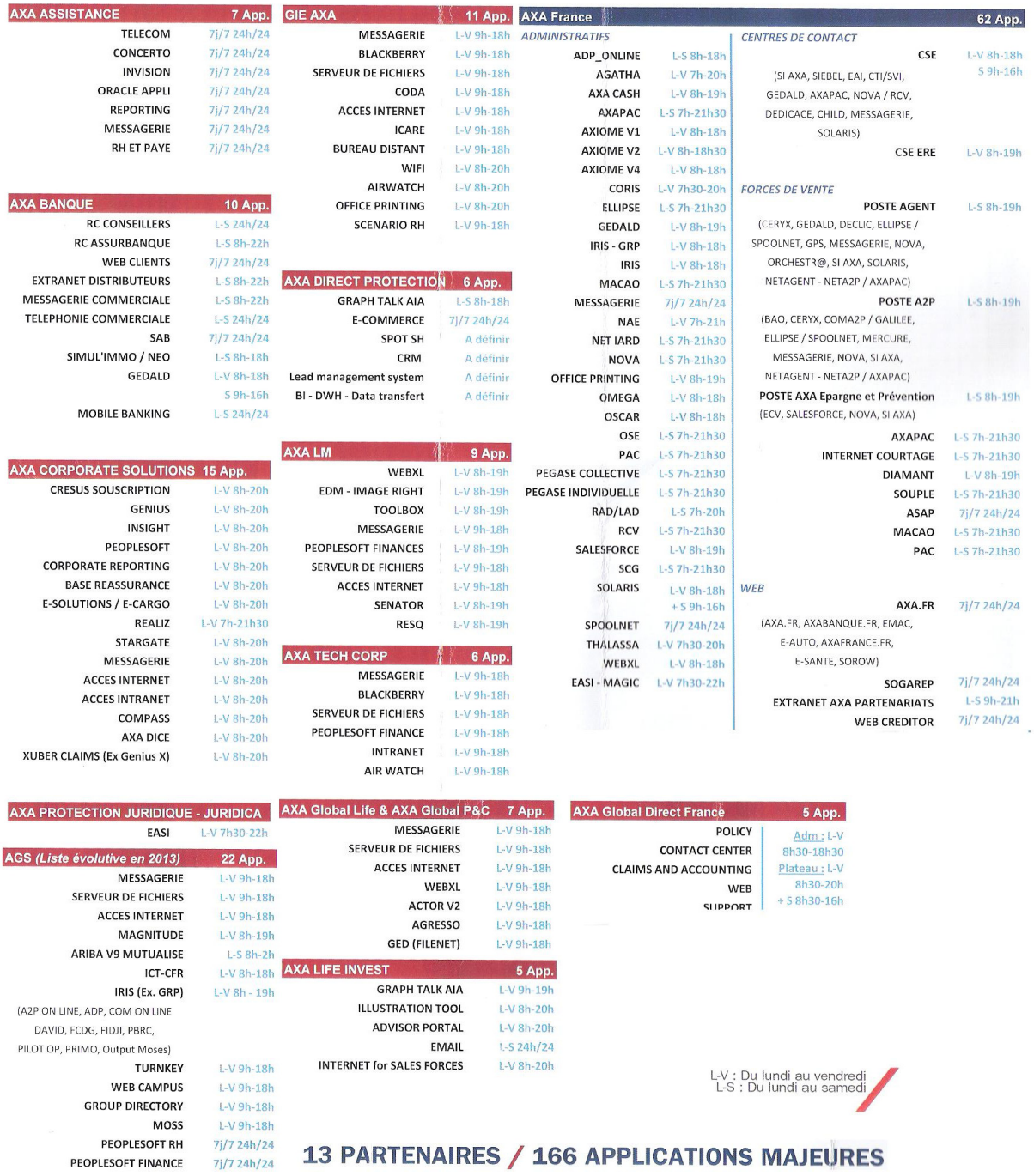
#Automatic Updates
SERVICE_NAME: wuauserv
SERVICE_ID:1

L'option «**NO_CHECK:**» permet d'exclure de la supervision d'un service une liste de contrôleurs de domaine. Dans ce cas, les contrôleurs de domaine seront séparés par un point virgule « **;** »

#PassGo Access Control Agent
SERVICE_NAME: MyPriAgent
NO_CHECK:PRINTSIEGDCLAG;PRINTSIEGDCK2;PRINTSIEGDCK1
SERVICE_ID:0

Pour exclure un seul serveur, l'option «**NO_CHECK:**» sera aussi utilisée.
#DNS Server
SERVICE_NAME: DNS
NO_CHECK:PRINTSIEGDCLAG
SERVICE_ID:0

Annexe 6 : La liste des partenaires et des applications majeurs



AXA ASSISTANCE	7 App.
TELECOM	7j/7 24h/24
CONCERTO	7j/7 24h/24
INVISION	7j/7 24h/24
ORACLE APPLI	7j/7 24h/24
REPORTING	7j/7 24h/24
MESSAGERIE	7j/7 24h/24
RH ET PAYE	7j/7 24h/24

AXA BANQUE	10 App.
RC CONSEILLERS	L-S 24h/24
RC ASSURBANQUE	L-S 8h-22h
WEB CLIENTS	7j/7 24h/24
EXTRANET DISTRIBUTEURS	L-S 8h-22h
MESSAGERIE COMMERCIALE	L-S 8h-22h
TELEPHONIE COMMERCIALE	L-S 24h/24
SAB	7j/7 24h/24
SIMUL'IMMO / NEO	L-S 8h-18h
GEDALD	L-V 8h-18h S 9h-16h
MOBILE BANKING	L-S 24h/24

AXA CORPORATE SOLUTIONS	15 App.
CRESUS SOUSCRIPTION	L-V 8h-20h
GENIUS	L-V 8h-20h
INSIGHT	L-V 8h-20h
PEOPLESOFT	L-V 8h-20h
CORPORATE REPORTING	L-V 8h-20h
BASE REASSURANCE	L-V 8h-20h
E-SOLUTIONS / E-CARGO	L-V 8h-20h
REALIZ	L-V 7h-21h30
STARGATE	L-V 8h-20h
MESSAGERIE	L-V 8h-20h
ACCES INTERNET	L-V 8h-20h
ACCES INTRANET	L-V 8h-20h
COMPASS	L-V 8h-20h
AXA DICE	L-V 8h-20h
XUBER CLAIMS (Ex Genius X)	L-V 8h-20h

AXA PROTECTION JURIDIQUE - JURIDICA	
EASI	L-V 7h30-22h

AGS *(Liste évolutive en 2013)*	22 App.
MESSAGERIE	L-V 9h-18h
SERVEUR DE FICHIERS	L-V 9h-18h
ACCES INTERNET	L-V 9h-18h
MAGNITUDE	L-V 8h-19h
ARIBA V9 MUTUALISE	L-S 8h-2h
ICT-CFR	L-V 8h-18h
IRIS (Ex. GRP)	L-V 8h - 19h
(A2P ON LINE, ADP, COM ON LINE DAVID, FCDG, FIDJI, PBRC, PILOT OP, PRIMO, Output Moses)	
TURNKEY	L-V 9h-18h
WEB CAMPUS	L-V 9h-18h
GROUP DIRECTORY	L-V 9h-18h
MOSS	L-V 9h-18h
PEOPLESOFT RH	7j/7 24h/24
PEOPLESOFT FINANCE	7j/7 24h/24

GIE AXA	11 App.
MESSAGERIE	L-V 9h-18h
BLACKBERRY	L-V 9h-18h
SERVEUR DE FICHIERS	L-V 9h-18h
CODA	L-V 9h-18h
ACCES INTERNET	L-V 9h-18h
ICARE	L-V 9h-18h
BUREAU DISTANT	L-V 9h-18h
WIFI	L-V 8h-20h
AIRWATCH	L-V 8h-20h
OFFICE PRINTING	L-V 8h-20h
SCENARIO RH	L-V 9h-18h

AXA DIRECT PROTECTION	6 App.
GRAPH TALK AIA	L-S 8h-18h
E-COMMERCE	7j/7 24h/24
SPOT SH	A définir
CRM	A définir
Lead management system	A définir
BI - DWH - Data transfert	A définir

AXA LM	9 App.
WEBXL	L-V 8h-19h
EDM - IMAGE RIGHT	L-V 8h-19h
TOOLBOX	L-V 8h-19h
MESSAGERIE	L-V 9h-18h
PEOPLESOFT FINANCES	L-V 8h-19h
SERVEUR DE FICHIERS	L-V 9h-18h
ACCES INTERNET	L-V 9h-18h
SENATOR	L-V 8h-19h
RESQ	L-V 8h-19h

AXA TECH CORP	6 App.
MESSAGERIE	L-V 9h-18h
BLACKBERRY	L-V 9h-18h
SERVEUR DE FICHIERS	L-V 9h-18h
PEOPLESOFT FINANCE	L-V 9h-18h
INTRANET	L-V 9h-18h
AIR WATCH	L-V 9h-18h

AXA France	62 App.
ADMINISTRATIFS	
ADP_ONLINE	L-S 8h-18h
AGATHA	L-V 7h-20h
AXA CASH	L-V 8h-19h
AXAPAC	L-S 7h-21h30
AXIOME V1	L-V 8h-18h
AXIOME V2	L-V 8h-18h30
AXIOME V4	L-V 8h-18h
CORIS	L-V 7h30-20h
ELLIPSE	L-S 7h-21h30
GEDALD	L-V 8h-19h
IRIS - GRP	L-V 8h-18h
IRIS	L-V 8h-18h
MACAO	L-S 7h-21h30
MESSAGERIE	7j/7 24h/24
NAE	L-V 7h-21h
NET IARD	L-S 7h-21h30
NOVA	L-S 7h-21h30
OFFICE PRINTING	L-V 8h-19h
OMEGA	L-V 8h-18h
OSCAR	L-V 8h-18h
OSE	L-S 7h-21h30
PAC	L-S 7h-21h30
PEGASE COLLECTIVE	L-S 7h-21h30
PEGASE INDIVIDUELLE	L-S 7h-21h30
RAD/LAD	L-S 7h-20h
RCV	L-S 7h-21h30
SALESFORCE	L-V 8h-19h
SCG	L-S 7h-21h30
SOLARIS	L-V 8h-18h + S 9h-16h
SPOOLNET	7j/7 24h/24
THALASSA	L-V 7h30-20h
WEBXL	L-V 8h-18h
EASI - MAGIC	L-V 7h30-22h
CENTRES DE CONTACT	
CSE	L-V 8h-18h S 9h-16h
(SI AXA, SIEBEL, EAI, CTI/SVI, GEDALD, AXAPAC, NOVA / RCV, DEDICACE, CHILD, MESSAGERIE, SOLARIS)	
CSE ERE	L-V 8h-19h
FORCES DE VENTE	
POSTE AGENT	L-S 8h-19h
(CERYX, GEDALD, DECLIC, ELLIPSE / SPOOLNET, GPS, MESSAGERIE, NOVA, ORCHESTR@, SI AXA, SOLARIS, NETAGENT - NETA2P / AXAPAC)	
POSTE A2P	L-S 8h-19h
(BAO, CERYX, COMA2P / GALILEE, ELLIPSE / SPOOLNET, MERCURE, MESSAGERIE, NOVA, SI AXA, NETAGENT - NETA2P / AXAPAC)	
POSTE AXA Epargne et Prévention	L-S 8h-19h
(ECV, SALESFORCE, NOVA, SI AXA)	
AXAPAC	L-S 7h-21h30
INTERNET COURTAGE	L-S 7h-21h30
DIAMANT	L-V 8h-19h
SOUPLE	L-S 7h-21h30
ASAP	7j/7 24h/24
MACAO	L-S 7h-21h30
PAC	L-S 7h-21h30
WEB	
AXA.FR	7j/7 24h/24
(AXA.FR, AXABANQUE.FR, EMAC, E-AUTO, AXAFRANCE.FR, E-SANTE, SOROW)	
SOGAREP	7j/7 24h/24
EXTRANET AXA PARTENARIATS	L-S 9h-21h
WEB CREDITOR	7j/7 24h/24

AXA Global Life & AXA Global P&C	7 App.
MESSAGERIE	L-V 9h-18h
SERVEUR DE FICHIERS	L-V 9h-18h
ACCES INTERNET	L-V 9h-18h
WEBXL	L-V 9h-18h
ACTOR V2	L-V 9h-18h
AGRESSO	L-V 9h-18h
GED (FILENET)	L-V 9h-18h

AXA LIFE INVEST	5 App.
GRAPH TALK AIA	L-V 9h-19h
ILLUSTRATION TOOL	L-V 8h-20h
ADVISOR PORTAL	L-V 8h-20h
EMAIL	L-S 24h/24
INTERNET for SALES FORCES	L-V 8h-20h

AXA Global Direct France	5 App.
POLICY	Adm : L-V 8h30-18h30 Plateau : L-V 8h30-20h + S 8h30-16h
CONTACT CENTER	
CLAIMS AND ACCOUNTING	
WEB	
SUPPORT	

L-V : Du lundi au vendredi
L-S : Du lundi au samedi

13 PARTENAIRES / 166 APPLICATIONS MAJEURES

Annexe 7 : Le lanceur GO_IVP.VBS

Le lanceur est un fichier dont l'extension est «.**vbs**». Il est éditable avec un éditeur de texte.

- **L'entête du script.**

```
'*************************************************************************
'**      Auto lanceur de scripts                                         *
'**      Version :       2.0                                             *
'**      Date de modification :          03-01-12                        *
'**      Auteur :        Rodrigue REGIS                                  *
'**      E-mail : rodrigue.regis@yahoo.fr                                *
'**     Demandeur : Olivier Manzano                                      *
'*************************************************************************
```

- **Définition des chemins d'accès aux différents programmes de la supervision**

```
rep= "..\"
config_rep="..\config\"
auth=rep&"AUTHENTIFICATION\PROD_AUTH_LDAP.vbs"
check_svc=rep&"CHECK_SERVICES\CHECK_SERVICES.VBS"
reponse_dns=rep&"TEST_REPONSE_DNS\SERVICES_DNS_NAME.vbs"
Check_joindomain=rep&"CHECK_SVC_JOINDOMAIN\PROD_AUTH_LDAP_SVC_Joindomain.vbs"
Check_dns=rep&"VERIF_ENREGISTREMENTS_DNS\CHECK_RECORDS_DNS.vbs"
```

- **Création des objets de type SHELL, nécessaire pour l'exécution des méthodes.**

Une méthode est une fonction qui permet d'être réutilisée sans avoir besoin la redéfinir. Il suffit de l' « évoquer », c'est-à-dire de n'initialiser pour l'utiliser. Dans l'exemple ci-dessous, je crée un objet du type shell qui permet d'évoquer la méthode « RUN ».

```
set WshShell=CreateObject("WScript.Shell")
```

- **Utilisation de la méthode RUN**

WshShell.Run **strCommand**,**intWindowStyle**,**bWaitOnReturn**

strCommand : Commande à exécuter

intWindowStyle : définit la taille et la position de la fenêtre de la commande

1 ➔Active et affiche une fenêtre

bWaitOnReturn : Spécifie si le système attend la fin de l'exécution pour exécuter les instructions suivantes :

True➔ attendre la fin de l'exécution de la commande

False➔ exécuter la commande et continuer sans attendre qu'elle se termine

```
WshShell.Run auth,1,true                ➔ test d'authentification
WshShell.Run check_svc,1,true           ➔ test des services Windows
WshShell.Run reponse_dns,1,true         ➔ test de la résolution de noms DNS
WshShell.Run check_joindomain,1,true    ➔ test du compte d'installation des serveurs
WshShell.Run Check_dns,1,true           ➔ vérification des enregistrements dans le DNS
```

Annexe 8 : La fonction MAIL pour la création du ticket de suivi

La fonction mail ci-deesous est issue du script de test d'authentification. C'est le même principe pour l'ensemble des autres programmes de la supervision. La seule différence se trouve dans « objEmail.Subject ». Mais il aurait pu être passé en paramètre à la fonction.

- **Création de la fonction mail**

Passage en argument, du domaine, du message contenant les contrôleurs de domaine défaillants et le nombre de contrôleurs de domaine défaillants

Function Mail(domaine,message,nb)

```
Set objEmail = CreateObject("CDO.Message")
objEmail.From = "wkldafa@axa-tech.com"
objEmail.To = mail_base
objEmail.Cc = Smtp_mailto
objEmail.Subject = "Authentification failed sur : " & nb & " DC du domaine : "& domaine
```

Formatage de la date et de l'heure, car elle est mal interprétée par l'application : 1/12/2012 ➔01/12/2012

```
if (Day(Date)<10) then
      jour="0" & Day(Date)
else
      jour=Day(Date)
end if
if (Month(Date)<10) then
          mois="0" & Month(Date)
else
          mois=Month(Date)
end if
if(Hour(Time) <10) then
          heure="0" & Hour(Time)
else
          heure= Hour(Time)
end if
if(Minute(Time) <10) then
          minutes="0" & Minute(Time)
else
          Minutes= Minute(Time)
end if
if(Second(Time) <10) then
      secondes="0" & Second(Time)
else
      secondes= Second(Time)
end if
```

Début de création des balises. Elles sont fournies au format texte par l'éditeur HP, mais nécessite de les adapter. Elles doivent être reformatées au format visual basic. Les variables sont intégrées dans les balises (en bleu).

```
    ObjEmail.Textbody = "<CreateTicket>" & VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<TICKETTYPE><![CDATA[incident]]></TICKETTYPE>"  &
VbCrLf
    ObjEmail.Textbody = ObjEmail.Textbody & "<CUSTOMER><![CDATA[SESD_INTERFACE,
GENERIC_NSM_CC(SIEGE.S000000)]]></CUSTOMER>" & VbCrLf
```

```
ObjEmail.Textbody = ObjEmail.Textbody & "<GROUP><![CDATA["& group_incident &
"]]></GROUP>" & VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<SUMMARY><![CDATA["&"Authentification failed sur : "
& nb & " DC du domaine : "& domaine&"]]></SUMMARY>" & VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<TYPE><![CDATA[incident ]]></TYPE>" & VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<IMPACT><![CDATA[3]]></IMPACT>" & VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<URGENCY><![CDATA[3]]></URGENCY>" & VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<SERVICE><![CDATA[ATS_SESD_BI_TWS SM.7
Interface]]></SERVICE>" & VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<REFNUMBER><![CDATA[]]></REFNUMBER>" &
VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<DESCRIPTION><![CDATA["& message &
"]]></DESCRIPTION>" & VbCrLf
objEmail.Textbody = objEmail.Textbody & "<SUBAREA><![CDATA[other]]></SUBAREA>" & vbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<AREA><![CDATA[data]]></AREA>" & VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<LOCATION><![CDATA[PARIS]]></LOCATION>" &
VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<AFFECTEDCI><![CDATA[]]></AFFECTEDCI>" &
VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "<STARTTIME><![CDATA["&Year(Date)&"/"& mois &
"/" & jour& " "  &  heure & ":" & minutes & ":" & secondes &"]]></STARTTIME>" & VbCrLf
objEmail.Textbody = objEmail.Textbody &
"<Z_IMAN_APPSYSTEM><![CDATA[testing1_appsystem]]></Z_IMAN_APPSYSTEM>" & vbCrLf
ObjEmail.Textbody = ObjEmail.Textbody &
"<Z_IMAN_JOBTRANS><![CDATA[testing2_jobtrans]]></Z_IMAN_JOBTRANS>" & VbCrLf
objEmail.Textbody = objEmail.Textbody &
"<Z_IMAN_ABEND_CODE><![CDATA[testing3_abendcode]]></Z_IMAN_ABEND_CODE>" & vbCrLf
ObjEmail.Textbody = ObjEmail.Textbody &
"<Z_IMAN_SYSTEM><![CDATA[testing4_system]]></Z_IMAN_SYSTEM>" & VbCrLf
objEmail.Textbody = objEmail.Textbody &
"<Z_IMAN_STEP_PGM><![CDATA[testing5_pgm]]></Z_IMAN_STEP_PGM>" & vbCrLf
ObjEmail.Textbody = ObjEmail.Textbody &
"<Z_IMAN_TRANS><![CDATA[testing6_trans]]></Z_IMAN_TRANS>" & VbCrLf
ObjEmail.Textbody = ObjEmail.Textbody & "</CreateTicket>" & VbCrLf
```

Méthode pour l'envoie de courriel avec visual basic script

- **SendUsing**: la valeur 2, pour l'envoi du message en utilisant le réseau.
- **SmtpServer**: nom du serveur SMTP.
- **SMTPServerPort**: port du serveur SMTP (par défaut : 25).

```
objEmail.Configuration.Fields.Item("http://schemas.microsoft.com/cdo/configuration/sendusing") = 2
objEmail.Configuration.Fields.Item("http://schemas.microsoft.com/cdo/configuration/smtpserver") =
smtp_serveur
objEmail.Configuration.Fields.Item("http://schemas.microsoft.com/cdo/configuration/smtpserverport") =
25
ObjEmail.Configuration.Fields.Update

On Error Resume Next
objEmail.Send
```

end function

Annexe 9 : lecture du fichier de configuration

Ci-dessous, un extrait du code source pour la lecture du fichier de configuration « config_ldap.ini

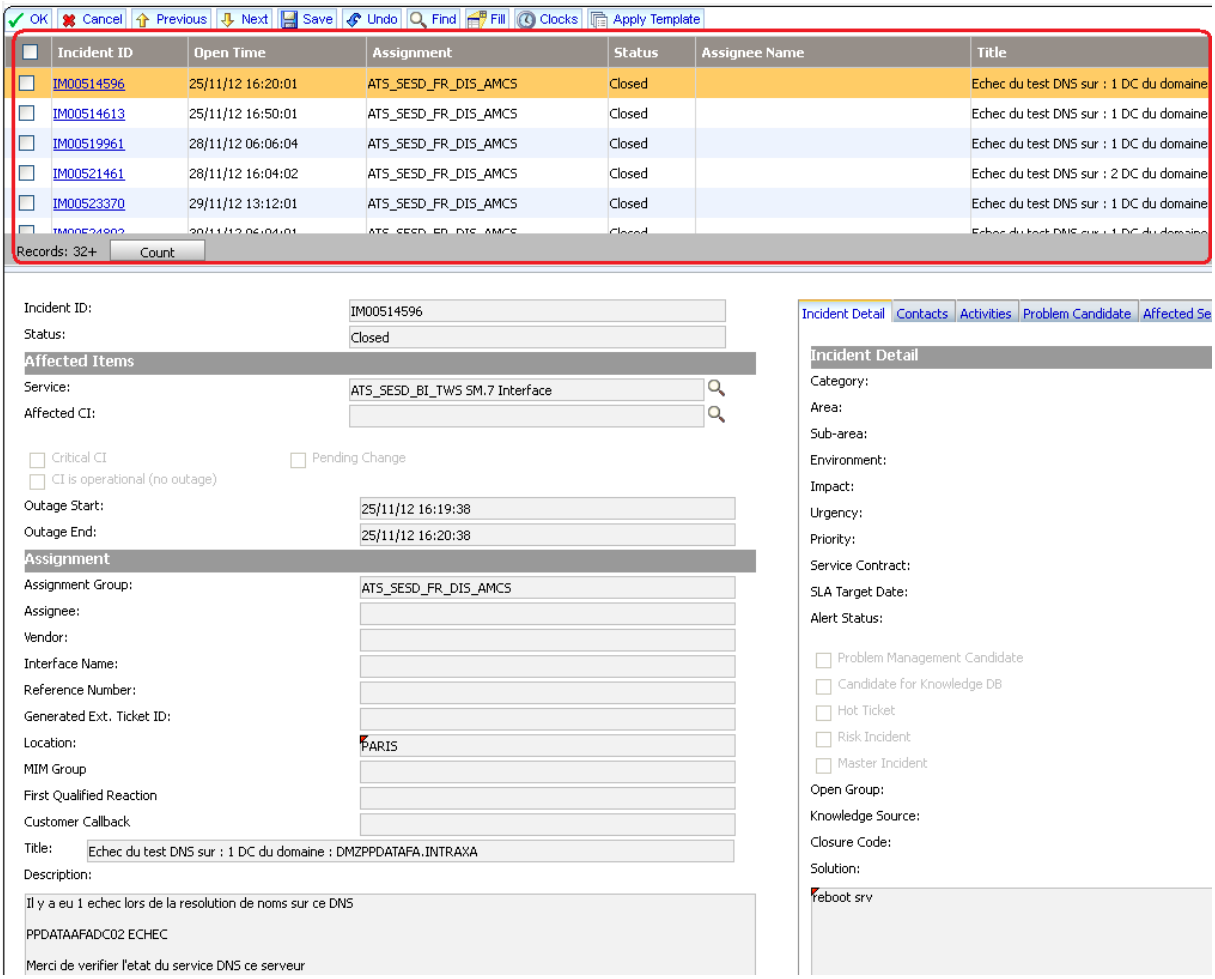
```
Const ForReading = 1, ForWriting = 2,ForAppend=8
config=config_rep&"config_ldap.ini"
Set fs = CreateObject("Scripting.FileSystemObject")
Set conf = fs.OpenTextFile(config, ForReading)

while Not conf.AtEndOfStream
        data = conf.ReadLine
    if( left(data,len("CHK_DOMAINE:"))="CHK_DOMAINE:") then
            strDomain=right(data,len(data)- len("CHK_DOMAINE:"))
            strDomain=replace(strDomain," ","")
    End If
    if( left(data,len("MAIL_BASE:"))="MAIL_BASE:") then
            mail_base=right(data,len(data)- Len("MAIL_BASE:"))
            mail_base=replace(mail_base," ","")
    End If
    if( left(data,len("GROUPE_INCIDENT:"))="GROUPE_INCIDENT:") then
            Group_incident=right(data,len(data)- Len("GROUPE_INCIDENT:"))
            Group_incident=replace(Group_incident," ","")
    End If
    if( left(data,len("NS_SERVEUR_NAME:"))="NS_SERVEUR_NAME:") then
            serveur_name(i)=right(data,len(data)- len("NS_SERVEUR_NAME:"))
    end if
     if( left(data,len("NS_SERVEUR_IP:"))="NS_SERVEUR_IP:") then
                dns(i)=right(data,len(data)- len("NS_SERVEUR_IP:"))
                i=i+1
    end if
    if( left(data,len("NS_DOMAINE:"))="NS_DOMAINE:") then
            domaine=right(data,len(data)- len("NS_DOMAINE:"))

    end if
    if( left(data,len("NS_CONTROLE_I:"))="NS_CONTROLE_I:") then
                controle_i(j)=right(data,len(data)- len("NS_CONTROLE_I:"))
                j=j+1
    end if
    if( left(data,len("NS_CONTROLE_N:"))="NS_CONTROLE_N:") then
                controle_n(j)=right(data,len(data)- len("NS_CONTROLE_N:"))
                controle_n(j)=Ucase(controle_n(j))
    end if
    if( left(data,len("NS_CONTROLE_A:"))="NS_CONTROLE_A:") then
                controle_a(j)=right(data,len(data)- len("NS_CONTROLE_A:"))
                t=t+1
    end if
    if( left(data,len("NS_DOMAINE_DC:"))="NS_DOMAINE_DC:") then
            ns_dc=right(data,len(data)- len("NS_DOMAINE_DC:"))
    end if
    if( left(data,len("SMTP:"))="SMTP:") then
            Smtp_serveur=right(data,len(data)- Len("SMTP:"))
            smtp_serveur=replace(smtp_serveur," ","")
    End If
    if( left(data,len("MAILTO:"))="MAILTO:") then
            Smtp_mailto=right(data,len(data)- Len("MAILTO:"))
            Smtp_mailto=replace(Smtp_mailto," ","")
    End If
Wend
```

Annexe 10 : Les incidents détectés par la supervision

Les tickets d'incidents créés dans la base de gestion des incidents d'ATS.



La supervision active directory

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

Résumé

L'active directory (AD) est un service d'annuaire distribué destiné aux entreprises. L'AD permet de se connecter aux ressources de l'entreprise. La supervision active directory a pour but de tester le fonctionnement de l'annuaire et d'alerter l'équipe support en cas d'incident.

AXA Technology Services(ATS) est une société filiale du groupe AXA. ATS gère l'infrastructure informatique d'AXA dans le monde. Après quelques incidents sur l'infrastructure active directory, ATS a souhaité renforcer la supervision sur l'ensemble de ses annuaires et regagner la confiance des utilisateurs.

La création d'un outil de supervision est présentée dans ce mémoire. La supervision fournit l'état de fonctionnement des contrôleurs de domaines, serveurs composants l'annuaire distribué. Elle crée des tickets de suivi dans la base de gestion des incidents pour une meilleure traçabilité.

Mots clés : active directory, annuaire, supervision, incident, ticket, traçabilité

Abstract

The active directory (AD) is a distributed directory service designed for enterprises. AD allows to connect to corporate resources. The AD monitoring aims to test reliability of the directory service and alert the technical support in case of incident.

AXA Technology Servces(ATS) is a subsidiary of AXA group company. ATS manages the IT infrastructure AXA in the world. After a few incidents on the active directory infrastructure, ATS has desired strengthen the monitoring on all of its directories and regain the trust of users.

The creation of a monitoring tool is presented in this thesis. Monitoring provides the operationnal status of all domain controllers, servers that are components of the distributed directory. It creates tickets in incident database for better traceability.

Key words : active directory, directory, monitoring,incident, tickets, traceability