Service Informatique

Ministères des Armées

2023

Date	Rédacteur	Validateur
19 février 2023	LE DOHER Loïc	

Table des matières

Présentation et déroulement du projet

Présentation du projet

Présentation du projet

- **Trois phases sont à distinguer dans la réalisation de cette intégration :**

Phase de préparation

➔ KICK OFF
➔ SC2A
➔ Etude des prérequis
➔ Etude des impacts sur le système (conception, maintenance et sauvegarde)
➔ Etude des impacts sur le réseau
➔ Définition de la solution d'hébergement
➔ Etude des impacts sur la SSI
➔ Etude des changements fonctionnels de l'administration technique de la solution

Phase de conception

➔ Changements fonctionnels et organisationnels dans l'utilisation de l'outil
➔ Production de la documentation d'installation
➔ STAGING: installation de la solution SVI sur les serveurs et test en environnement de pré-production.

Mise en Production

➔ Mise en réseau des serveurs et ouverture aux utilisateurs des nouveaux services
➔ Production d'un document de tests prédéfini entre le Ministère et l'industrielle en prévision de la recette de la solution
➔ Conception de la documentation fonctionnelle (guide d'utilisation, plan de formation)
➔ Politique du changement

Le rôle de l'administrateur dans ce projet est de s'assurer de l'adéquation du produit et de la cible visée, avec la cohérence technique du Ministère des Armées.

Qu'est-ce que le serveur vocal interactif ?

Le SVI est une technologie de téléphonie qui permet aux clients d'une entreprise d'interagir avec son système téléphonique via des menus vocaux.

Il remplace un réceptionniste dans la majeure partie des cas, car il est capable donner des renseignements de manière automatique (par exemple sur les horaire d'ouverture de service) et permet également de proposer des messages avec choix multiples, afin d'aiguiller un appel pour une meilleure expérience client.

- **Comment ?**

Les correspondants se voient proposer un choix pour sélectionner des options en appuyant sur les touches du clavier de leur téléphone (les dernières versions du SVI permettent également de choisir vocalement ces options). Ce routage, appelé « CALL FLOW » s'appuient sur des messages préenregistrés, des séquences de questions et des actions à réaliser en fonction des choix faits par l'appelant (Annexe 2).

Il est à noter qu'avec la mise en place de la nouvelle version du SVI, il a été décidé de refondre totalement les « CALL FLOW » déjà existants. En effet, le routage actuel ne proposait que deux aiguillages, l'un pour les VIP VOP (résolution d'incidents prioritaires), et l'autre pour les utilisateurs « standards ».

- **Pourquoi ?**

Le serveur vocal permet de gérer et entretenir un volume important d'appels téléphoniques, d'acheminer ces derniers vers les ressources techniques les plus appropriées, et d'établir des statistiques sur le volume et la qualité des réponses apportées aux besoins d'interventions sur l'outil informatiques, qu'il concerne le domaine bureautique ou les applications métiers.

- **Les avantages pour le Ministère :**

Disponibilité permanente : le SVI assure l'accueil des utilisateurs en H24.

Economiser les ressources humaines : le gain de productivité et réduction des coûts opérationnels : l'aiguillage des utilisateurs étant automatique le SVI sollicite moins de ressources pour la gestion d'appels entrants.

Amélioration de l'image perçue du service : la qualité de réponse et son ciblage étant améliorée, l'utilisateur aura une impression positive du service rendu.

- **Les avantages pour l'utilisateur :**

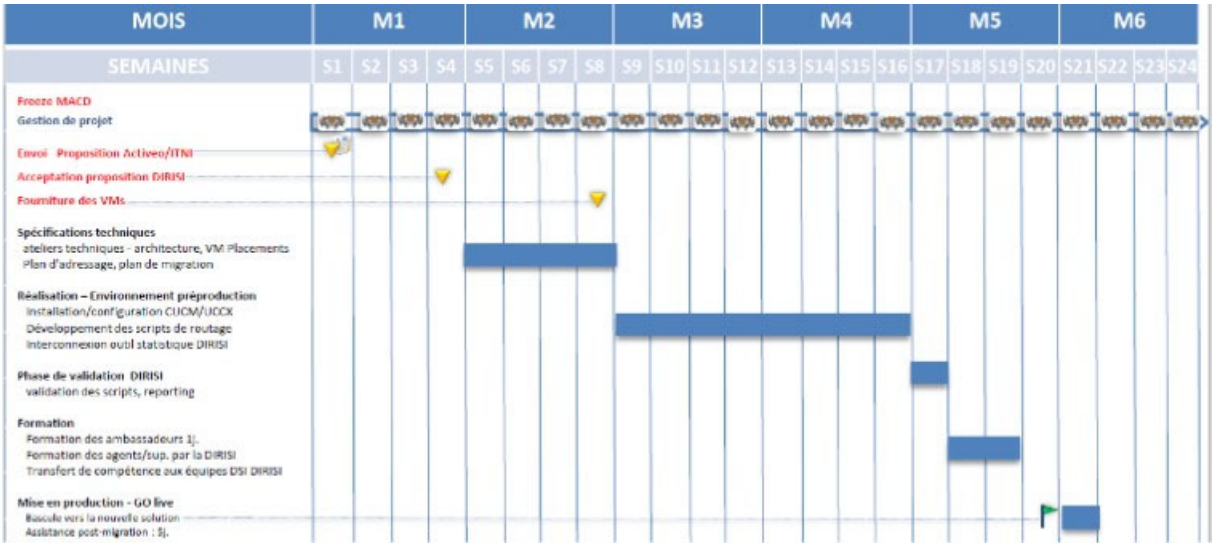
L'amélioration de l'expérience client grâce à l'aiguillage automatique ou suite à ses choix effectués.

Prise en charge et résolution des problèmes plus rapide car l'utilisateur est immédiatement redirigé vers l'opérateur ou le service le plus à même de répondre à sa demande.

Méthodologie du projet :

Dans le cadre de la gestion de projet SVI et du respect des délais des différentes étapes de son déroulement, l'outil adopté fût le « diagramme de GANTT » (voir annexe 1)

Planning prévisionnel :



- **Macro-planning du projet :**

  - Conception du projet 01/2022 : Etude des prérequis, et impacts. Validation SC2A.
  - Conception : Installation et configuration des serveurs en 02/2022 (Staging)
  - Déploiement mi-2022 – Début de la réorganisation fonctionnelle.
  - Documentations techniques et fonctionnelles en 06/2022 – Début des formations.
  - Mise en production 09/2022

- **Points d'étapes :**
  - Réunion hebdomadaire « Coproj » les Mardis matin pour le suivi détaillé des tâches à effectuer et validation de celle qui ont été effectuées (avec mise à jour du planning de départ).
  - Réunions trimestrielles en présentiel avec tous les acteurs du projet, afin de valider les décisions concernant des variations éventuelles sur les orientations initiales du projet.

À la suite de ces réunions, le récapitulatif des informations et des sujets traités sont partagés sur un espace de travail collaboratif SharePoint, sur lequel les parties prenantes au projet peuvent consulter et déposer toute documentation utile au projet (Annexe 3).

Parties prenantes au projet :

- **L'équipe ACTIVEO/ITNI** : un commercial /chef de projet et un technicien administration. Ils représentent la partie des intervenants externes du projet (intégrateurs).
- **Pôle conduite de projet** ➔ Chef de projet.
- **Pôle Opérationnel Espace Numérique de Travail (POENT)** ➔ Administrateur technique.
- **L'équipe Back Office du SDK Maisons-Laffitte** : Directeur SDK, administrateurs fonctionnels
- **Le Pole Opérationnel hébergement (POHEB)** ➔ réalise l'analyse technique du besoin en hébergement et prépare ce dernier.
- **Le Pôle Opérationnel Sécurité Administration (POSA)** ➔ SSI en interne, il organise la maintenance de l'outil dans l'avenir
- **L'équipe Réseau (RDTM)** ➔ En charge de l'architecture réseau.
- **Le Pôle supervision du Ministère** ➔ En charge de la supervision Système et Réseau.
- **Pole opérationnel réseau transport et desserte (POLE RTD)** ➔ assure le fonctionnement général de l'organisme et exerce ses prérogatives dans les domaines des ressources humaines, des finances, des achats, de la comptabilité, de la maîtrise des risques, de la sécurité et de l'infrastructure.
- **Société Anaya** ➔ Audit externe SSI (action annexe, réalisée sur demande du service SSI du Ministère, aux fins d'obtenir des conseils pour le « durcissement » de la solution.)
-

Le POSA est en charge de l'exploitation et de la fourniture des services SIC de l'infrastructure numérique sous la responsabilité de la DIRISI dans les domaines de l'administration et de la sécurité.
Il est chargé :

- De piloter et de coordonner les prestations d'exploitation délivrées par la DIRISI,
- D'exploiter des réseaux et systèmes confiés à la DIRISI,
- D'assurer la conduite de l'activité des centres techniques
- De garantir la permanence des liaisons entre les systèmes d'information et de communication d'infrastructure du Ministère de la défense.

- **L'équipe Réseau (RDTM)** ➔ En charge de l'architecture réseau.
- **Le Pôle supervision du Ministère** ➔ En charge de la supervision Système et Réseau.
- **Pole opérationnel réseau transport et desserte (POLE RTD)** ➔ assure le fonctionnement général de l'organisme et exerce ses prérogatives dans les domaines des ressources humaines, des finances, des achats, de la comptabilité, de la maîtrise des risques, de la sécurité et de l'infrastructure.
- **Société Anaya** ➔ Audit externe SSI (action annexe, réalisée sur demande du service SSI du Ministère, aux fins d'obtenir des conseils pour le « durcissement » de la solution.)

Cahier des charges :

Afin de réaliser le projet d'intégration du SVI, il a été établi le cahier des charges suivant :

- **Solution actuelle :**

Solution de téléphonie : Cisco Call Manager v.11.5 (10 serveurs).

Solution de centre d'appel : Cisco Unified Contact Center Enterprise v.11.5 (14 serveurs).

Neuf passerelles voix (routeurs) ancienne génération, qui permettent l'interconnexion avec l'opérateur ou le réseau téléphonique interne.

- **Contenu de la nouvelle solution :**

Quatre serveurs Cisco Unified Call Manager (CUCM) v.14 dédiés pour le système de téléphonie sur IP et la gestion des IP Phones Cisco

Deux serveurs Cisco Unified Contact Center Express (UCCX) v.12.6 dédiés pour le système de centre d'appels et la gestion du bandeau agent

Un serveur Cisco Satellite dédié pour la gestion des licences Cisco

Un serveur Logepal dédié pour l'affichage des statistiques du centre d'appels sur des écrans de contrôle grand format.

Deux machines dédiées à l'exploitation de la solution

Neuf passerelles voix (routeurs) nouvelle génération, qui permettent l'interconnexion avec l'opérateur ou le réseau téléphonique interne.

- **Cible :**

  - Mise à jour la solution de téléphonie Cisco Call Manager dans la dernière version 14
  - Remplacement de la solution UCCE en UCCX express version 12.6
  - Utilisation de 2 serveurs virtuels, avec nécessité de deux fois moins de vCPU, de RAM, et de disques par serveur.
  - Architecture centralisée de la solution
  - MAJ futures du S.I. moins complexe
  - Aucune perte fonctionnelle par rapport aux usages actuels sur UCCE
  - Remplacement des passerelles voix (routeurs VOIP)
  - Refonte de la sécurisation du S.I.
  - Simplification des actions de maintenance technique.
  - Mise en place d'une supervision du système.

- **La solution répondra également aux besoins fonctionnels de la DIRISI, à savoir :**

Accompagner les utilisateurs et les exploitants afin de faciliter le changement

Migrer les utilisateurs vers le nouveau système de téléphonie et de centre d'appel en générant le moins de perturbations possibles pour ces utilisateurs finaux.

Fournir une solution plus moderne d'un centre de services (Service Desk), dans le but de fournir un soutien et de l'assistance aux usagers du Ministère de la Défense.

Fournir des scripts de routage correspondant aux nouveaux besoins des SDK en termes de qualité de service rendu.

Simplification de l'administration fonctionnelle.

- **Moyens :**

Financiers : Coût de l'opération intégré dans le plan de charge financier de la DIRISI en 2020.
Humains : Chaque service impliqué dans ce projet devra désigner un correspondant privilégié, chargé de l'exécution par ses équipes, des actions ordonnées par le chef de projet. Les parties prenantes externes (ITNI, ACTIVEO), devront fournir les ressources nécessaires à la configuration, la mise en pré-production et en production, l'établissement des livrables, ainsi qu'aux actions de formations induites par le projet.

- **Livrables documentaires attendus :**

Le dossier de spécifications techniques (format Excel).
Les documentations techniques et fonctionnelles
Le cahier de tests et de recette technique (format Excel).
Les documents de formation pour les opérateurs/superviseurs/administrateurs fonctionnels (Finesse, CUIC, CC Care).
Les documents de formation à l'exploitation de l'UCCX et du CUCM nouvelle version pour les administrateurs techniques. Le mode opératoire de la migration.

En résumé, le projet consiste à mettre en œuvre une version à jour du SVI, plus légère et plus performante toute en respectant les standards informatiques en vigueur au sein du Ministère. La DIRISI souhaite également atteindre un niveau fonctionnel plus élevé, avec des routages d'appels plus pertinents que ceux déjà existants.

Problématique :

Le projet SVI n'étant pas un simple projet de mise à jour logiciel, mais une refonte totale de ce S.I., les problèmes que nous pourrions potentiellement rencontrer lors de la conduite de celui-ci peuvent être multiples :

- La solution est-elle intégrable à notre SI général ?
- Correspond-elle aux prérequis de notre politique d'hébergement (matériel et architectural) ?
- Respecte-t-elle les usages SSI du Ministère ?
- A contrario, le Ministère offre-t-il les prérequis de base demandés par CISCO pour le bon fonctionnement de sa solution SVI ?
- A isopérimètre la nouvelle solution propose-t-elle à minima le même fonctionnement que la solution existante ? (Perte de fonctionnalités ?).
- Combien de temps et quelles ressources pourront-être allouées pour l'étude de la mise en œuvre de cette solution, par chaque acteur à ce projet : réseaux, hébergement, SSI, intervenant externe, utilisateurs etc… ?
- Une formation supplémentaire (au niveau administrateurs techniques) devra être ajoutée aux formations déjà prévues.

Phase de Préparation

La première étape dans la phase de préparation fût la tenue d'une réunion appelée « KICKOFF » qui réunit d'une part: les représentants des sociétés ACTIVEO-ITNI et d'autre part les experts techniques du Ministère des Armées concernés par le projet.
Le but de cette réunion était de confirmer la cible à atteindre ainsi que les prérequis majeurs :

- Identifier définitivement les différents acteurs prenant part au projet
- Etablir une méthode de travail commune avec des documents communs
- Etablir le 1 er planning prévisionnel

A la suite de cette réunion « Kick Off », la 1 ère mission des administrateurs techniques a été de compléter un document appelé SC2A. Il décrit précisément, toutes les caractéristiques d'architecture du nouveau SI. Il est à présenter au Sous- Comité de Cohérence des architectures.


MINISTÈRE DES ARMÉES
SC²A
Sous-Comité de Cohérence des Architectures
MIGRATION SVI VER. 14 ET UCCX
Date : 28/01/2022
Type de demande

- Ce Sous-Comité, en respectant le référentiel du cadre de cohérence technique :
- Emet des conseils et avis relatifs à l'architecture ou au choix de solutions techniques.
- Assiste et oriente les directions d'applications dans la définition de leur architecture et le choix des composants logiciels et matériels.
- Valide ou non, les architectures des nouveaux systèmes d'informations proposés, sur la base du dossier SC2A.

Dans le cas d'une validation du projet décrit dans le SC2A par le Sous-Comité, la conception du projet peut continuer.
Dans un premier temps, il faut étudier les prérequis (du constructeur et du Ministère) nécessaires à la mise en place de ce S.I.
Les Prérequis constructeur nécessaires à la mise en place du nouveau SVI :

- Matériel : Actuellement les VMs du centre d'appel sont installées sur des serveurs LENOVO System x3550 M5 avec des CPU Intel XEON ex-2630 V4 @2.20Ghz et cette référence de CPU n'est plus compatible avec la solution CISCO 14. Il est donc nécessaire de changer le matériel pour une version plus performante avec une puissance minimale de 2.50 GHz (fréquence de base) pour le bon fonctionnement du SI.
- Réseau : la bande passante minimum est à paramétrer. La QOS, importante pour la VOIP, exige que les paquets arrivent dans l'ordre et donc avec des priorités de transfert.
- Hyperviseurs : La répartition des ressources n'est plus la même puisque le nombre de VMs est diminué. (Voir schéma 1.2)
- Les versions ESXI : les versions supportées sont les versions 6.5 ou 7.5, avec tous les updates et patchs installés.
- Téléphones : Les téléphones compatibles sont : Cisco 6921 et 7962G.
- Licences : Les licences CISCO seront injectées sur les serveurs de manière manuelle (les liens vers l'extérieur n'étant pas autorisées pour des questions de sécurité)
- Navigateur et OS : Windows 10 pour les stations de travail. Les navigateurs compatibles avec le bandeau Finesse sont : Internet Explorer 11, Firefox 68 ESR, Chrome et Microsoft Edge.

Les Prérequis du Ministère nécessaires à la mise en place du nouveau SVI :

- Matériels : Correspondre aux standards matériels utilisés par les services informatiques du Ministère.
- Logiciel : N'utiliser que des piles logicielles autorisées par les architectes système et la SSI du Ministère (notamment concernant les niveaux de version à minima).
- SSI : Répondre aux standards de sécurité édictés par les services SSI du Ministère (matrice des flux acceptable, type de communication entre les différentes briques du système contrôlable, possibilité de supervision avancée, politique de sauvegarde prévue, gestion des logs, gestion des accès à privilèges élevés). Une étude est automatiquement initiée en interne, en même temps que la phase de préparation, en vue d'une homologation du projet par la SSI. Un questionnaire dédié est obligatoirement complété par le chef de projet, afin de déterminer quel type d'homologation sera retenu (standard ou simplifié).

Dans un second temps, il faut s'attacher à mettre en lumière les impacts de cette migration sur l'architecture système existante

Architecture système actuelle

Les serveurs sont disposés sur les sites du Mont Valérien et de Rennes, (un serveurs ESXI physique sur chaque site).
La solution actuelle est composée :

- D'une solution de téléphonie : Cisco Call Manager v.11.5 sur 5 serveurs virtuels
- D'une solution de centre d'appel : Cisco Unified Contact Center Enterprise v.11 sur 19 serveurs virtuels

Schéma 1.1

A ce jour, les statistiques d'utilisation de ce S.I. sont les suivantes (statistiques observées sur la pile UCCE) :

- Agents déclarés : 689
- Nombre d'agents connectés simultanément : 100
- Nombre de licences UCCE : 400 (licences comptées sur le nombre de postes téléphoniques déclarés comme « enrôlés » sur le système)

Architecture système cible

Au vu des statistiques d'utilisation décrites plus haut concernant l'UCCE, il n'est pas justifié de prolonger ce type d'architecture. La solution UCCX, plus simple, suffit largement au besoin de la DIRISI. Description de la solution UCCX :

- Cette solution supporte jusqu'à 400 communications en simultanées (alors qu'aujourd'hui la solution UCCE ne permettait qu'un maximum de 118 communications simultanées).
- Elle est mieux sécurisée.
- Elle supporte mieux la Haute disponibilité.
- L'administration technique est simplifiée.
- L'administration fonctionnelle est simplifiée.
- Le Bandeau téléphonie sur poste de travail est plus intuitif pour les agents et les superviseurs.

Avantages	Inconvénients
• Utilisation de 2 serveurs virtuels pour l'UCCX • Consommation de 2 fois moins de vCPU, RAM, Disque qu'une solution UCCE • Aucune licence Windows ni SQL n'est nécessaire (attention, uniquement pour la partie UCCX) • Plus de patch Windows ni d'antivirus • Architecture centralisée identique à celle en production • Intégration et migration moins complexe • Aucune perte fonctionnelle par rapport à l'UCCE • Exploitation simplifiée avec CCCare	• Pas de possibilité d'export des statistiques.

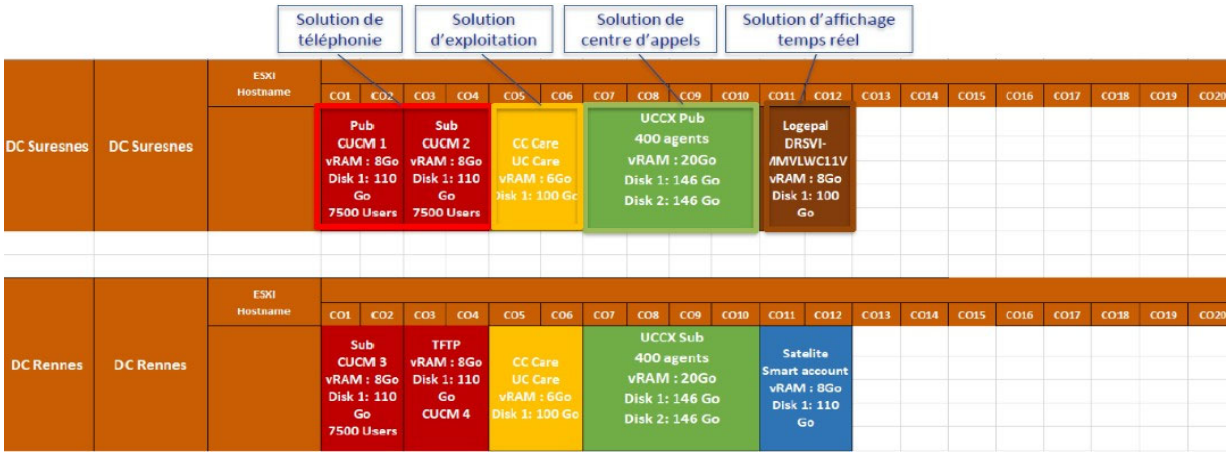
Les nouveaux serveurs seront aussi disposés sur les sites du Mont Valérien et de Rennes, (un serveur ESXI sur chaque site).
La nouvelle solution est composée de :

- Quatre VMs Cisco Unified Call Manager dédiées au système de téléphonie sur IP et à la gestion des IP Phones Cisco
- Deux VMs Cisco Unified Contact Center Express (UCCX) dédiées au système de centre d'appels et la gestion du bandeau agent
- Deux VMs UC Care pour l'exploitation de la solution de centre d'appels Calibri Light ?
- Une VMs Dédiée à l'administration des licences.
- Une VMs Logepal dédiée à l'affichage des statistiques du centre d'appels sur des écrans de contrôle.

Type	Produit	Version	Statut CCT (E,R,A[1],D,I,-)	Soutien (E,S,O,N,-)[2]	Observations
Call manager (Cisco Unified Call Manager)	CUCM OS : centos BDD : informix	14.0SU1 7.0.0.0-7 64bits 12.10.UC13X3	- D -	- - -	Appliance Cisco où tout est packagé.
Cisco Unified Contact Center Express	UCCX OS : centos BDD : informix	12.5(1)SU01_ES02 7.0.0.0-7 64bits 12.10.UC9W1X3	- D -	- - -	Appliance Cisco où tout est packagé.
Application UC CARE (provisionning CUCM et UCCX)	UCCARE OS : Windows Server BDD : SQL Server	4.4.2.6 WS2016 standard 2014 ou 2016	- R R	- S S	Produit Activeo
Application Logepal (Gestion des affichages)	Logepal OS : Windows BDD : SQL	6.3.10.12 WS2016 standard 2014 ou 2106	- R R	- S S	Produit Activeo

L'aménagement des nouveaux serveurs virtuels est le suivant :

Schéma 1.2

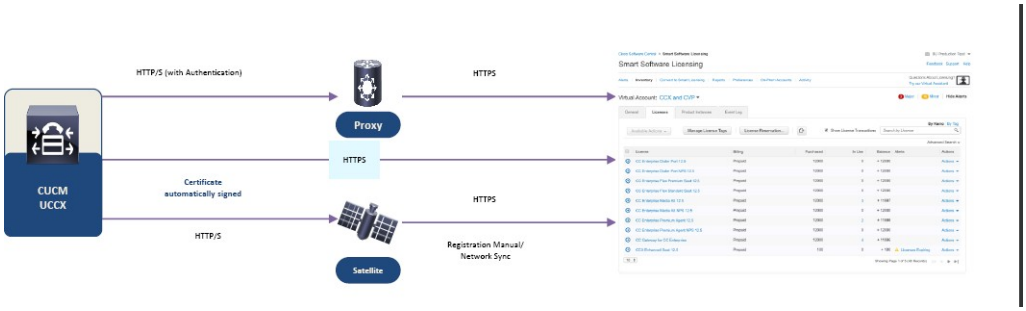


Pour information, concernant la gestion des licences :

La société ITNI avait soumis dans sa proposition la gestion des licences agents via sa solution : Smart Software Licensing. Avec une communication sécurisée avec Cisco smart licensing :

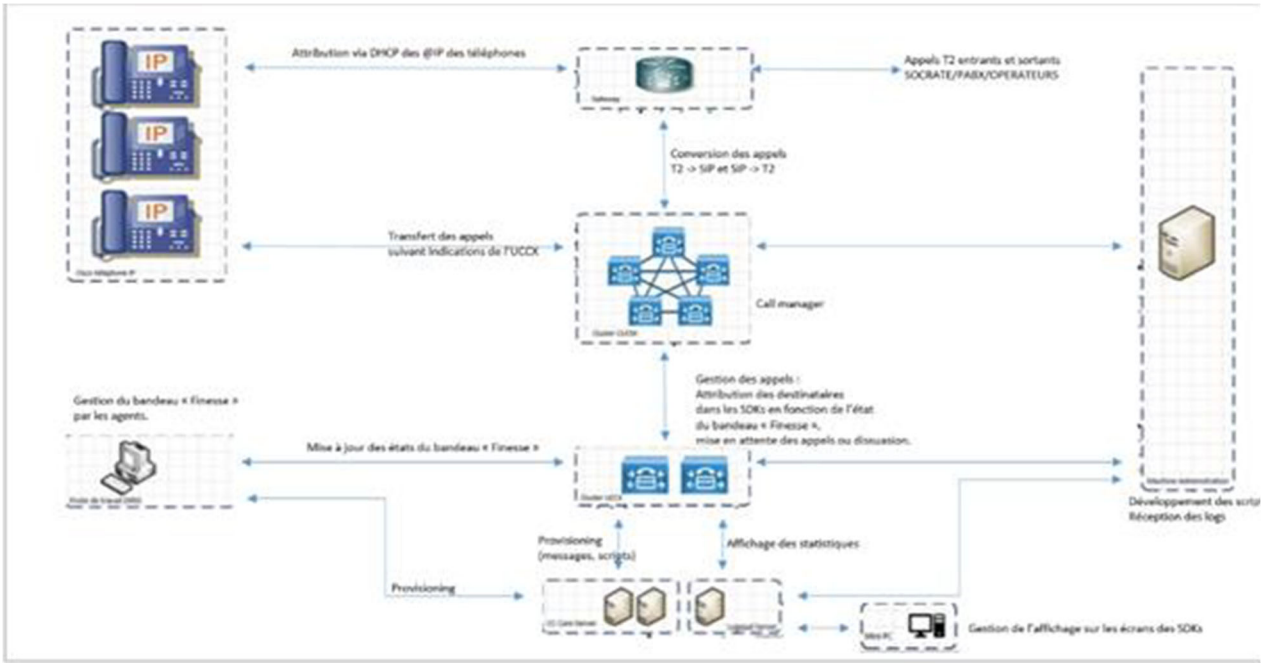
1. En se connectant au cloud Cisco via un proxy
2. Via un serveur satellite

Ces deux propositions ont été refusées, puisqu'il n'est pas autorisé pour les réseaux de la Défense de se connecter sur le Cloud Cisco en vue de récupérer et/ou activer les licences des applications concernées. Les licences seront mises à jour « manuellement » après leur récupération sur le site Cisco.



En ce qui concerne la maintenance, les mises à jour des VM Cisco demandant la compétence d'un partenaire certifié, elles seront réalisées par l'intégrateur. Les équipes des SDK assureront leur provisioning et leur monitoring. Les serveurs UC Care, ADM et Logepal nécessitent des mises à jour des OS Windows et des antivirus ainsi que des sauvegardes périodiques. Ces points seront également abordés plus loin dans ce document, lors de la description du choix du type d'hébergement effectué par le Ministère pour ce SVI.

Ce changement d'Architecture système amène donc un changement dans l'architecture physique générale du SVI :

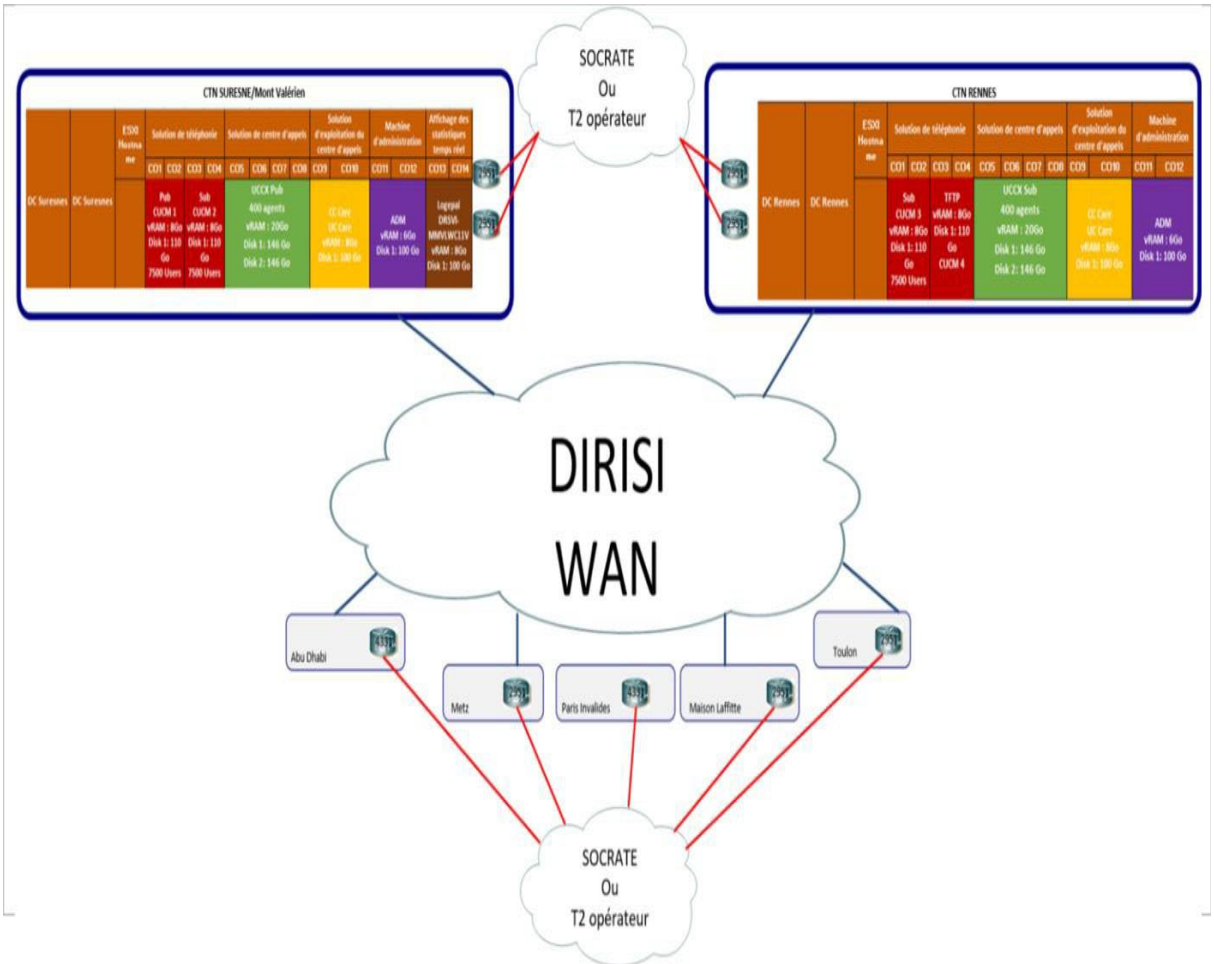


Architecture réseau du nouveau SVI :

L'architecture réseau ne change pas significativement.
Il est tout de même à noter que les adresses IP utilisées par nouveau le S.I. changeront, mais sur une plage d'adresse en /24 déjà utilisée par l'ancienne version du SVI.

Comme mentionné précédemment, les routeurs VOIP servant de passerelle vers les opérateurs extérieurs ou les le réseau téléphonique interne à l'organisation (SOCRATE) seront modernisés, mais ne seront pas déplacés dans l'architecture existante. Le reste des transferts de données IP et VOIP sera fait, comme auparavant, via le WAN du Ministère.

Schéma 1.3



Changement fonctionnel de l'administration de la solution

Le choix de l'hébergement, conditionnera le type d'administration de la solution.
Comparatif des différentes offres d'hébergement du Ministère :

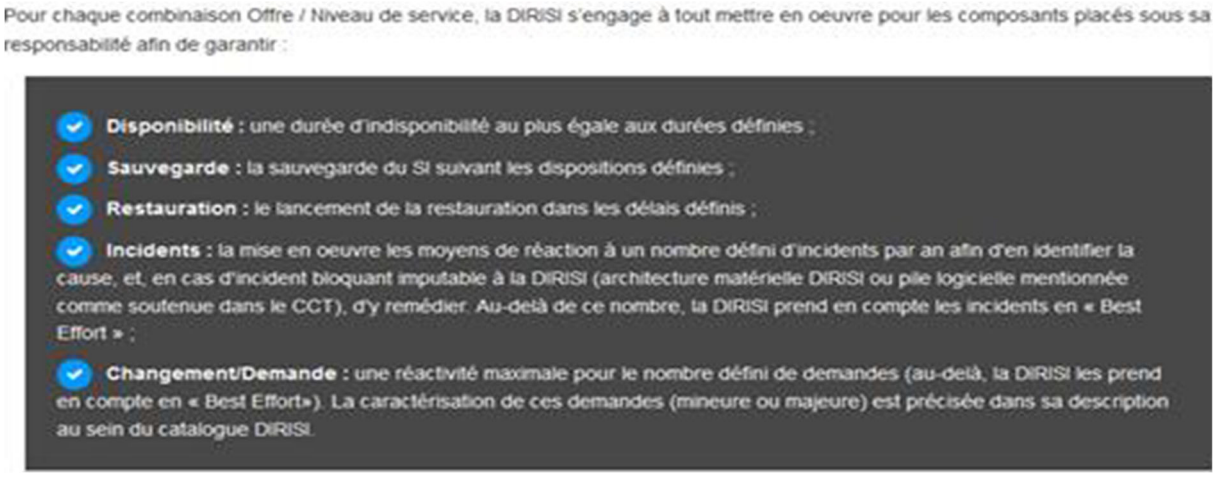
- **Salle Blanche :** Les serveurs physiques sont fournis par la DIRISI dans le cadre du projet de migration, les mises à jour des OS Windows et antivirus, les sauvegardes ainsi que l'exploitation sont réalisées par les exploitants des SDK.

- **VPS et Infogérance :** Le Pôle Hébergement met à disposition des VM dans le Datacenter, si le besoin de machines physiques apparaît, leur fourniture est à leur charge. Dans ce cas, seules les opérations d'exploitation restent à la charge des SDK, les mises à jour et les sauvegardes sont traitées par le POHEB.

  Inconvénients : Les machines physiques fournies par le Pôle Hébergement peuvent ne pas répondre aux prérequis Cisco, ce qui est rédhibitoire pour le MCO de la solution

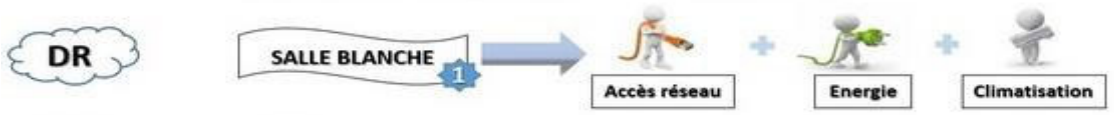
- **Mixte des deux offres salle Blanche et VPS** : les VM en salle blanche concernent les applications de téléphonie et de contact center Cisco, les autres VM nécessitant un OS Windows sont intégrées dans l'offre VPS.

  Inconvénients : Le fait que les serveurs soient répartis sur deux types d'hébergements différents complexifiera la mise en œuvre réseau et la résolution de problème en cas d'incident.



La décision du choix d'hébergement

Pour notre SI le type d'hébergement se rapprochant au plus de nos besoins, et préconisé dans le SC2A est la Salle Blanche :



Salle Blanche	Les serveurs sont commandés par le projet et répondent aux prérequis Cisco.	- Les exploitants du SDK devront à la fois traiter les mises à jour des systèmes Windows et de la solution d'antivirus ainsi que les sauvegardes en supplément de leur activité d'exploitation du centre de contact.

Nous disposons de nos serveurs dans le cadre du projet de migration, les mises à jour des OS Windows et antivirus, les sauvegardes ainsi que l'exploitation sont réalisées par nos équipes. Nous devrons cependant définir de qui incombera l'infogérance.

Les prestations de la DIRISI consistent dans cet hébergement uniquement en la fourniture d'un emplacement au sein d'une architecture matérielle DIRISI existante, dans une salle serveur climatisée avec accès aux réseaux électriques et informatiques. Le matériel fourni doit obligatoirement être compatible avec la structure. En cas de défaillance, nous disposons du service d'infogérance à minima

	Offre « SALLE BLANCHE »			
Domaine	**Niveau de service « BRONZE »**	**Niveau de service « ARGENT »**	**Niveau de service « OR »**	**Niveau de service « PLATINE »**
Disponibilité	24h d'indisponibilité par mois sur la plage horaire de service (HO)	12h d'indisponibilité par mois sur la plage horaire de service (HO)	12h d'indisponibilité par mois sur la plage horaire de service (HO/HNO) PCI mis en place par le demandeur	4h d'indisponibilité par mois sur la plage horaire de service (HO/HNO) PCI mis en place par le demandeur
	96h totales d'indisponibilité par an en cas de crash Hardware majeur de l'infrastructure DIRISI (hors restaurations)	72h totales d'indisponibilité par an en cas de crash Hardware majeur de l'infrastructure DIRISI (hors restaurations)	36h totales d'indisponibilité par an en cas de crash Hardware majeur de l'infrastructure DIRISI (hors restaurations)	12h totales d'indisponibilité par an en cas de crash Hardware majeur de l'infrastructure DIRISI (hors restaurations)
	L'indisponibilité ne concerne que les équipements sous la responsabilité de la DIRISI, à savoir la climatisation, l'énergie, le réseau (hors équipement fourni par le Bénéficiaire. *Le périmètre de l'engagement ne comprend pas les indisponibilités pour opération de maintenance planifiée.)*			
Changement / Demande	Au plus 1 demande d'intervention (hors traitement d'un incident) par trimestre (en HO) par le Bénéficiaire, sur ses équipements et avec accompagnement de la DIRISI	Au plus 1 demande d'intervention (hors traitement d'un incident) par mois (en HO) par le Bénéficiaire, sur ses équipements et avec accompagnement de la DIRISI	Au plus 1 demande d'intervention (hors traitement d'un incident) par cuinzaine (en HO) par le Bénéficiaire, sur ses équipements et avec accompagnement de la DIRISI	Au plus 1 demande d'intervention (hors traitement d'un incident) par semaine (en HO) par le Bénéficiaire, sur ses équipements et avec accompagnement de la DIRISI

Le choix de l'administrateur technique s'est porté sur le POENT et celui de l'administrateur fonctionnel sur le SDK.
Les différentes sauvegardes des données système (configuration, BDD, machines virtuelles), seront prise en charge par l'un des serveurs robot du Ministère dédié à cette tâche.

Changement organisationnel dans l'utilisation de l'outil, aspect SSI.

Il faut maintenant aborder l'aspect organisationnel, notamment du point de vue de la sécurité et les questions soulevée par ces différents changements d'architecture.
Il a été décidé de réaliser un audit sur ce point, réalisé en parallèle, par les services SSI du Ministère, et la société ANAYA sur la décision RSSI :
Cette mission se compose de trois audits différents :

- **Un audit d'architecture :** L'audit d'architecture consiste en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériel et logiciels déployés dans un système d'information, à l'état de l'art et aux exigences et règles internes.

Au cours de la réunion de lancement des ateliers SSI, nous validons ensemble le périmètre, la documentation à utiliser, la méthode d'audit, les interlocuteurs à contacter, le calendrier et les livrables

Analyse des informations et documents recueillis à la suite de la réunion de lancement

Entretiens avec les différentes parties prenantes

Investigations techniques ;

Formalisation des résultats des analyses dans un rapport, exposant également des recommandations de remédiations

- **Un audit d'organisation :** L'audit organisationnel comprend un diagnostic qui débouche sur l'identification des vulnérabilités et des risques associés et permet de formuler des recommandations visant à améliorer la sécurité de l'organisation. Celles-ci seront explicitées et priorisées dans un plan d'actions.

- **Un audit technique de configuration :** L'audit de configuration permet de vérifier la mise en œuvre de pratiques de sécurité conformes à l'état de l'art et aux exigences et règles internes de sécurité. L'audit portera sur les configurations des dispositifs matériels et logiciels déployés dans le SVI.

L'audit de configuration se déroulera selon les phases suivantes :

- Réunion de lancement avec les parties prenantes, au cours de laquelle nous validons ensemble le périmètre, la documentation à utiliser, la méthode d'audit, les interlocuteurs à contacter, le calendrier et les livrables
- Analyse des informations et documents recueillis lors de la réunion de lancement
- Investigations techniques sur les configurations des briques du SI pour évaluer le respect des bonnes pratiques de sécurisation des différents composants du socle, des infrastructures et des logiciels.
- Etude des surfaces d'attaques possible :
    - Exposition Interne : En interne peu probable (MDP robuste)
    - Exposition Externe : ouverture du S.I sur réseau, accessibilité et dimensionnement. Niveau des impacts :
        - L'importance des activités sur tout le Ministère
        - Conséquence indirecte d'un incident sur le SI

Cet audit a donc pour objectif déterminer les principaux points faibles du SI. Il sera précédé d'une réunion de lancement de la mission avec toutes les parties prenantes. La mission sera finalisée par une réunion de restitution et de synthèse globale. Ci-après, un extrait des points à étudier.

Risque	Occurrence	Impact	Solution apportée
Panne d'un serveur physique	Faible	Très faible	Redondance MLV/RNS
Désactivation d'une VM Cisco	Faible	Très faible	Redondance des VMs
Arrêt d'une VM UCCare	Faible	Nul	Pas de criticité sur le fonctionnement du SVI, re-synchoniser les VM entre les sites
Arrêt de la VM Logepal	Faible	Coupure de l'affichage	Pas de criticité sur le fonctionnement du SVI, au besoin restaurer une sauvegarde de l'application.
Coupure de lien entre les sites de MVL et de RNS	Faible	Voir Youssef	Sécurisation des liens à mettre en place entre les DC de MVL et de RNS
Mauvaise gestion de la QoS	Inconnu	Fort	Dégradation de la voix

Risque	Occurrence	Impact	Solution apportée
Panne d'une passerelle voix	Faible	Faible sur les appels entrants, à qualifier sur les appels sortants (voir Youssef)	Redondance sur les appels entrants avec le groupement de lignes.
Coupure ligne opérateur	Faible	Faible sur les appels entrants, à qualifier sur les appels sortants (voir Youssef)	Redondance sur les appels entrants avec le groupement de lignes.
Téléphone pirate	Faible	Très faible	Le serveur DHCP n'attribue des adresses qu'aux téléphones déclarés.

Le système SVI proposé par CISCO étant complexe mais adaptable en termes de configuration, il a été décidé que cet audit pouvait se dérouler en même temps que la phase de conception et la mise en production.

Le durcissement éventuel des éléments audités pourra être réalisé à posteriori de la mise en production.

La solution la plus probable selon les premiers éléments constatés par les parties prenantes à cette étude, serait de créer une DMZ propre au SVI qui permettrait par l'intermédiaire d'un ou plusieurs firewalls de surveiller les flux entrants et sortant (à minima blocage des flux non autorisés).

L'idée n'étant pas de faire du firewalling niveau 7, mais au niveau 3, car les paquets arrivant de l'extérieur ont déjà été analysés par différents protocoles de sécurité existants sur le réseau.

Je précise que l'audit n'était pas terminé à mon départ du Ministère

Un aspect de la sécurité qui en revanche, a pu être conceptualisé et mis en place rapidement fût la supervision du système.

La Supervision :

La solution de supervision utilisée pour une majeure partie des systèmes informatiques du Ministère est le service PISARO fondé sur la solution Shinken Entreprise (elle-même étant une amélioration de la solution libre Centreon). L'accès au service se fait sur un portail dédié géré par « l'Administrateur Shinken » (Annexe 4).

Le service permet la surveillance matérielle, applicative et du la qualité service rendu, afin de permettre aux techniciens, aux superviseurs, et au commandement, d'être informés en temps réel de l'état des services dont ils ont la charge.

La supervision du matériel est à la charge de l'administrateur technique du SI.

En ce qui concerne le SVI, des « templates » de supervision type ont été directement appliqués sur les serveurs windows du système. Pour les serveurs « CISCO », les Mibs et OIDs pertinentes ont été demandées au constructeur, afin de créer une supervision adaptée.

Changement organisationnelle dans l'utilisation et l'administration de l'outil

Au niveau organisationnel, l'arrivée de la nouvelle version du SI remet en question le périmètre d'intervention des administrateurs système et fonctionnel du SVI sur les plans de l'administration des serveurs, la maintenance et l'évolution des fonctionnalités offertes par le produit, la supervision, les mises à jour Windows et Cisco ainsi que la sauvegarde.

Exemples problématiques SSI relevées au niveau organisationnel :

L'hébergement en salle blanche nécessite la désignation de référent habilité pour le SI. La question qui se pose est de savoir à qui incombe la responsabilité des mises à jour Windows ainsi que des mises à jour antivirus ? En ce qui concerne les mises à jour de sécurités Windows obligatoire nous pouvons les installer automatiquement mais concernant les MAJ « Frameworks » il sera impératif de les effectuer en accord avec l'industriel, ce dernier devant avoir un accès physique aux baies serveurs, afin de travailler directement sur les piles logicielles.

Phase de conception – Le Staging

À la suite de la validation du document SCD2A nous pouvons désormais démarrer la configuration de bases des serveurs de RENNES et SURESNES.

Durant la phase dite « STAGING » et à l'aide de la documentation d'installation que nous avons validé au préalable avec l'intégrateur nous avons procédé avec le technicien, à la configuration des serveurs.

Cette action a été effectuée dans un environnement de pré-production simulant le réseau de production. Ce type de staging a été rendu obligatoire par le fait que les serveurs Cisco devaient obligatoirement communiquer avec un serveur DNS et NTP pour s'installer.

- **Création du RAID**

Définition du RAID : C'est une technologie qui permet de se servir de plusieurs disques durs à la fois et de les réunir comme une seule entité logique avec la possibilité de stocker les données sur plusieurs disques durs mais en les utilisant comme s'il s'agissait d'un seul et unique support

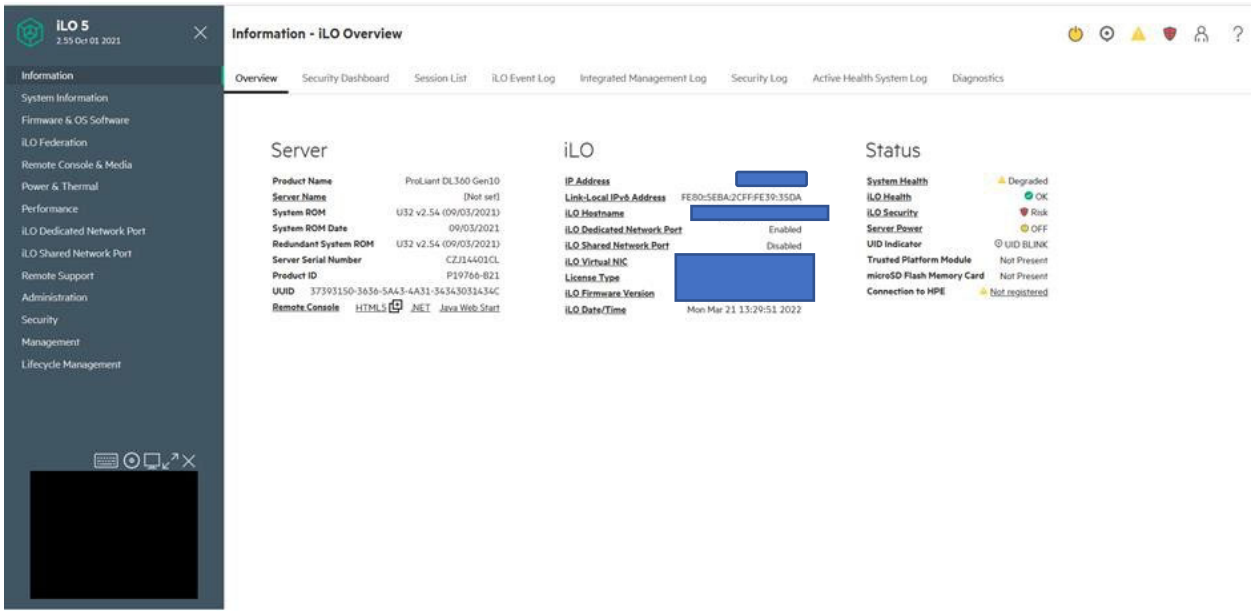
Pourquoi le fait-on ? Pour gagner en vitesse de lecture et d'écriture et minimiser dans notre cas les risques de pertes de données en cas de pannes.

Avant l'installation des ESXI, dans un premier temps nous avons créé le RAID 5, pour se faire je me suis connectée au premier serveur. A partir de son BIOS je configure la taille du Raid que je souhaite monter ce qui permettra d'avoir l'espace disponible restant pour le spare. Dans notre cas nous avons 8 disques dont 1 spare.

A l'étape suivante, nous avons vérifié à l'aide des lumières LED lequel de ces disques est le Spare (disque de secours) qui offrira une protection supplémentaire contre la perte de données.

Dans notre cas le disque est inutilisé et ne stocke aucune donnée, si l'un des disques du groupe RAID tombe en panne il remplacera automatiquement le disque défectueux. (Reconstruction du RAID)

Le Raid est maintenant monté, nous testons l'administration à distance du serveur en se connectant à la carte ILO > Console à distance sur le même réseau que serveur via l'interface WEB.



- **Installation des serveurs Windows 2016 :**

1 Pour CCare -> installation du système de gestion de bdd MsSQL (Microsoft SQL server) + création d'un compte root local + compte SA (uniquement pour l'installation) après installation nous créerons des comptes fonctionnels.

1 Logepal -> Installation de MsSql Express (version gratuite) avec une capacité limitée supportant des bdd d'une taille de 10 Go maximum. Installation de MsSql tools à installer pour le Management studio afin de permettre d'accéder, configurer, gérer, administrer et développer les composants de SQL server en interface graphique.

1 serveur d'administration pour la gestion des serveurs.

- **Installation de UCCX et UCCM - récupération de la BDD existante concernant la téléphonie** (n°/nom/référence du tel)

- **Configuration des serveurs de Rennes et Suresnes terminé**

Tests effectués :

➔ Connexion au serveur physique via interface web ILO (annexe p.39)

➔ Connexion SSH sur chaque interface CISCO serveur

➔ Connexion accès au ESXI via Interface Web

➔ Connection via connexion à distance aux serveurs Windows

Les interfaces ont bien toutes été vérifiés et sont fonctionnelles avant la mise en place dans le Datacenter. Si, à la mise en production, il est détecté un problème de communication au serveur nous pourrons suspecter une mauvaise configuration au niveau réseau supérieur ou d'un firewall.

Transfère de la base de données existante sur SRV

Parallèlement, nous avons sauvegardé la base de données du SVI en production afin de pouvoir l'injecter plus tard dans le nouveau système. Cette première sauvegarde ne constitue pas une étape de « FREEZE » de l'administration de la solution mais simplement d'un 1er test d'injection sur la nouvelle base de données afin de détecter des anomalies.

Le staging est maintenant fini, nous procédons à présent à l'installation des serveurs physiques dans les baies de production (cela ne veut pas dire qu'ils rentrent en production). A ce stade il reste à tester le bon fonctionnement réseau et système de la solution après ces vérifications viendront les phases de FREEZE de la BDD et d'implémentation des briques fonctionnels.

La demande d'intégration au domaine n'étant pas automatique, nous avons dû faire la faire via NEMO (nouvelle messagerie officielle) au POSA qui donnera son aval pour l'intégration au domaine mais aussi dans une OU dédiée (OU existante ou création). Pour exemple, dans le cadre notre projet le POSA a décidé de créer une OU métier spécifique dans le domaine INTRADEF.

La demande de création de compte de service dédiée à ce SI ainsi que la déclaration officielle des comptes administratifs qui sont utilisés lors de la mise en production du SVI seront aussi rattachés au NEMO précité.

Pour finir cette action, un cahier de tests sera proposé par Activeo, pour validation par la DIRISI. Si tous ces tests effectués sont concluants, la phase de mise en production peut commencer.

Mise en production

- **Les formations et la documentation technique**.

En préambule de la description de la mise en production, il est important de mentionner l'aspect formation et production de documentions d'exploitation technique et fonctionnelle (annexe 5) qui incombe à l'intégrateur dans le cadre du contrat qu'il a passé avec le Ministère.

En ce qui concerne la documentation technique, elle doit reprendre de manière exhaustive toutes les informations concernant l'architecture réseau et système du SVI ainsi que les procédures utilisées lors de l'installation de ce dernier.

Concernant les formations, 4 type de sessions sont prévus :

➔ Administrateurs techniques.

➔ Administrateurs fonctionnels

➔ Chefs de plateau

➔ Opérateurs

Ces formations devront être effectués pour la plupart de ces agents, avant la mise en production.
A partir de la présentation du produit, la DIRISI procédera à la distribution de planche de communications résumant les nouvelles fonctions du SVI.
Ces planches sont destinées à présenter les changements apportés par la mise à jour du SI mais surtout mettre en avant la plus-value apportée par les nouvelles fonctions présentes dans la nouvelle version.

- **Le plan de mise en production**

Je précise, qu'à mon départ du Ministère des Armées, la mise en production n'était pas encore lancée. En revanche, il a été décidé que le plan de mise en production s'articulera principalement sur :

- Le listing de toute les actions à effectuer pour une mise en production complète et fonctionnelle
- La création d'un plan de mise en production technique (le basculement réseaux et systèmes) afin de minimiser l'impact de cette action sur la disponibilité du SI.
- L'injection des BDD
- La migration des passerelles avec changement de configuration des routeurs VOIP
- La vérification du bon fonctionnement (système et réseau des nouveaux serveurs SVI)
- La vérification du bon fonctionnement des postes d'administration ainsi que les postes de travail et téléphoniques reliés au SVI
- La vérification des logs sur les serveurs (log sur l'observateur d'événement Windows et/ou sur l'interface web ILO Cisco)
- La vérification du bon fonctionnement des nouveaux scripts de routage des appels
- L'analyse des risques de perte de service et mise en place d'une stratégie de Roll back en cas d'échec de la bascule.

Pour information : Des tests ont été déjà effectués durant la phase de préproduction (conception) pour permettre d'éliminer le plus d'erreur possible avant la mise en production.