BTS Services informatiques aux organisations- SISR

Session 2025

E5 – Support et mise à disposition de services informatiques

Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat :

Nathan VANDENBOSSCHE

Contexte de la réalisation professionnelle

- ***Layer Bureautique et Informatique*** *est une entreprise spécialisée dans la gestion d'infrastructures IT et la virtualisation, offrant des services essentiels pour répondre aux besoins de performance, sécurité et continuité des systèmes informatiques de ses clients.*
- *La problématique principale réside dans la nécessité de garantir la disponibilité et la sécurité des services informatiques tout en assurant la mise à jour et l'optimisation des infrastructures, sans compromettre la continuité des activités.*
- *La solution choisie consiste à effectuer une mise à jour progressive et contrôlée des serveurs vSphere et ESXi, et migrations de VMs via vMotion pour assurer la continuité des services pendant les interventions.*

Intitulé de la réalisation professionnelle

Gestion des Mises à Jour VMware : Garantir la Performance et la Sécurité des Infrastructures IT

Période de réalisation : 10/06/24- 14/06/24 **Lieu :** Auxerre

Modalité : ☒ Individuelle ☐ En équipe

Principale(s) activité(s) concernée(s) :

- ORGANISER SON DEVELOPPEMENT PROFESSIONNEL
- REPONDRE AUX INCIDENTS ET AUX DEMANDES D'ASSISTANCE ET EVOLUTION

Conditions de réalisation

- **Ressources présentes (situation avant la RP)**

  L'infrastructure de nos clients comprend plusieurs hôtes ESXi, ce qui limite la migration à chaud des VMs, et des systèmes non mis à jour, exposant l'environnement à des vulnérabilités.

- **Résultats attendus (situation après la RP)**

  Après la mise à jour, l'infrastructure sera entièrement à jour avec les derniers correctifs de sécurité. La migration des VMs effectuée sans interruption de service, garantissant ainsi une continuité totale des opérations.

- **Durée de réalisation**

  La réalisation de la mise à jour et de la migration est estimée à une demi-journée, à condition de ne pas rencontrer de problèmes. Cependant, sur certaines infrastructures, j'ai parfois rencontré divers problèmes qui ont prolongé la durée à une journée.

Modalités d'accès à cette réalisation professionnelle.

https://portfolio.vdb-pro.fr *mdp : Cyb3r-M@P89$*

Partie 1 – Procédure de mise en œuvre

Dans le cadre de ma mission chez **Layer Bureautique et Informatique**, j'ai été chargé de mettre à jour l'infrastructure VMware de l'entreprise. Cette intervention vise à renforcer la sécurité et la performance des systèmes pour garantir aux clients une continuité de service optimale et une protection accrue contre les vulnérabilités. Mon objectif est de mener à bien cette mise à jour tout en minimisant l'impact sur les opérations courantes, en suivant les meilleures pratiques de migration et de maintenance pour chaque composant essentiel de l'infrastructure.

Répondre aux incidents et aux demandes d'assistance et d'évolution

Lorsqu'une faille de sécurité est détectée dans le cadre de notre veille informatique, il est impératif de la traiter rapidement en la considérant comme un incident. Nous commençons par contacter les clients concernés, un par un, afin de leur expliquer clairement la nature de la faille, les risques encourus, et de leur proposer une solution immédiate : le déploiement d'une mise à jour corrective.

Chaque intervention fait alors l'objet de la création d'un **ticket d'incident** dans notre système de gestion interne, **LAYER**. Ces tickets sont initialement ouverts par un manager, puis intégrés dans ce que nous appelons le **"PIPE"** — une file d'attente ou une liste de tâches dédiée aux techniciens.

Étant formé aux mises à jour sur les environnements **VMware**, les demandes liées à ces interventions m'ont été assignées. J'ai donc pris en charge les tickets correspondants dans mon PIPE. Cela inclut la prise de contact avec les clients pour obtenir leur accord, planifier l'intervention, et procéder aux mises à jour nécessaires.

Une fois l'intervention terminée, il est essentiel de rédiger un **compte rendu détaillé**, qui est ensuite transmis au client. Ce rapport permet de garantir une transparence totale sur les actions réalisées et de maintenir une traçabilité complète des modifications apportées à leur infrastructure.

Communication avec les clients concernant les vulnérabilités

Nous contactons nos clients susceptibles d'être vulnérables aux nouvelles failles de sécurité. Pour assurer un suivi optimal, nous utilisons un tableau répertoriant toutes les versions des équipements et logiciels utilisés par nos clients. Cela nous permet de cibler rapidement ceux qui nécessitent une attention particulière.

Ensuite, nous prenons contact par téléphone pour leur expliquer la nature de la vulnérabilité à laquelle ils sont exposés et les informer de la nécessité d'effectuer une mise à jour. Il est de notre devoir de tenir nos clients informés des risques potentiels. Nous avons également la responsabilité de les inciter à effectuer ces mises à jour afin d'éviter tout problème futur.

En agissant ainsi, nous contribuons à renforcer la sécurité de leurs infrastructures et à prévenir d'éventuelles attaques.

Prérequis

Avant d'entamer les mises à jour, certains prérequis sont indispensables pour assurer leur bon déroulement et éviter tout dysfonctionnement. Voici les étapes à respecter :

1. Libérer les hôtes ESXi :
   Assurez-vous que les hôtes ESXi ne contiennent aucune machine virtuelle (VM) active. Si des VMs sont présentes, elles doivent être éteintes avant toute intervention. Mettre les hôtes ESXi en mode maintenance.
2. Migration des VMs :

   Pour assurer la continuité de la production, il est essentiel de migrer les VMs d'un hôte ESXi à un autre. Cette migration doit être effectuée dans le respect des ressources disponibles sur les hôtes ESXi cibles, qui doivent être suffisantes pour accueillir les VMs migrées.

   Il est également possible d'éteindre certaines VMs qui ne seront pas utilisées ou qui n'affecteront pas la production, à condition d'obtenir au préalable l'accord du client. Cette approche permet d'optimiser l'utilisation des ressources.
3. Accès aux hôtes ESXi :
   Il est primordial d'avoir un accès sécurisé aux hôtes ESXi, soit via un VPN, soit en étant sur site, ou encore en se connectant à un serveur physique tel que les serveurs VEEAM, afin de prendre la main sur le vCenter.
4. vCenter opérationnel :
   Le vCenter doit être correctement configuré, avec tous les hôtes ESXi montés et le kernel vMotion soit bien configurés pour permettre une migration fluide des VMs.

5. Gestion des sauvegardes :

Si VEEAM est virtualisé, il est crucial de désactiver temporairement les sauvegardes pendant l'opération. De plus, veillez à vérifier les dispositifs de sauvegarde physique tels que les lecteurs LTO ou RDX pour éviter toute interruption ou conflit.

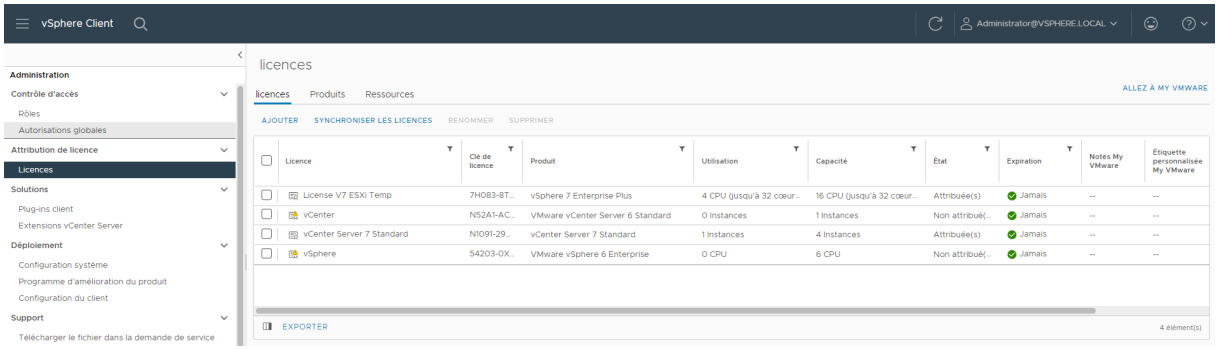
J'ai donc été chargé d'assurer la mise à jour complète de l'infrastructure VMware des entreprises. Cela inclut le vCenter, les hôtes ESXi et les machines virtuelles (VMs). C'est une tâche cruciale car elle garantit que tout l'environnement fonctionne avec les dernières sécurités et fonctionnalités, sans interruption pour les utilisateurs finaux.

Accès et vérification initiale des licences

Je commence par me connecter au **vSphere Client** via le FQDN. L'interface me permet d'avoir un aperçu rapide de toutes les VM en fonctionnement. Pour préparer la mise à jour, je dois d'abord m'assurer que toutes les licences sont valides. Mais avant de toucher aux licences, je fais une capture d'écran de l'état actuel des VM et de leur configuration de démarrage automatique. Cela me permettra de tout remettre en ordre une fois la mise à jour terminée.

Problème avec les licences vSphere 7 Essentials :

En accédant à la gestion des licences, je découvre que l'entreprise utilise une version **vSphere 7 Essentials**, qui ne permet pas la migration à chaud des VMs via **vMotion**. Cela pose un défi, car je dois migrer les VMs avant de mettre à jour les ESXi sans arrêter les machines en production.



Dans le cas où le client n'aurait pas les bonnes licences pour migrer, je prends alors l'initiative de récupérer des licences temporaires plus complètes depuis notre vCenter. Après avoir navigué dans **Administration > Licences**, je copie les clés nécessaires.

Une fois les licences récupérées, je retourne sur le vCenter du client et ajoute les nouvelles licences dans l'onglet **Administration > Licences**. Je les renomme en **TEMPORAIRE ESXi MAJ LAYER** et **TEMPORAIRE VCSA MAJ LAYER**, puis j'attribue les licences respectivement au vCenter et aux hôtes ESXi.

Configuration du vMotion

Pour faciliter la migration des VMs, j'active le **vMotion** sur l'adaptateur VMkernel des ESXi. Ce service me permet de déplacer les VMs d'un hôte ESXi à un autre sans interruption, ce qui est indispensable pendant la mise à jour.

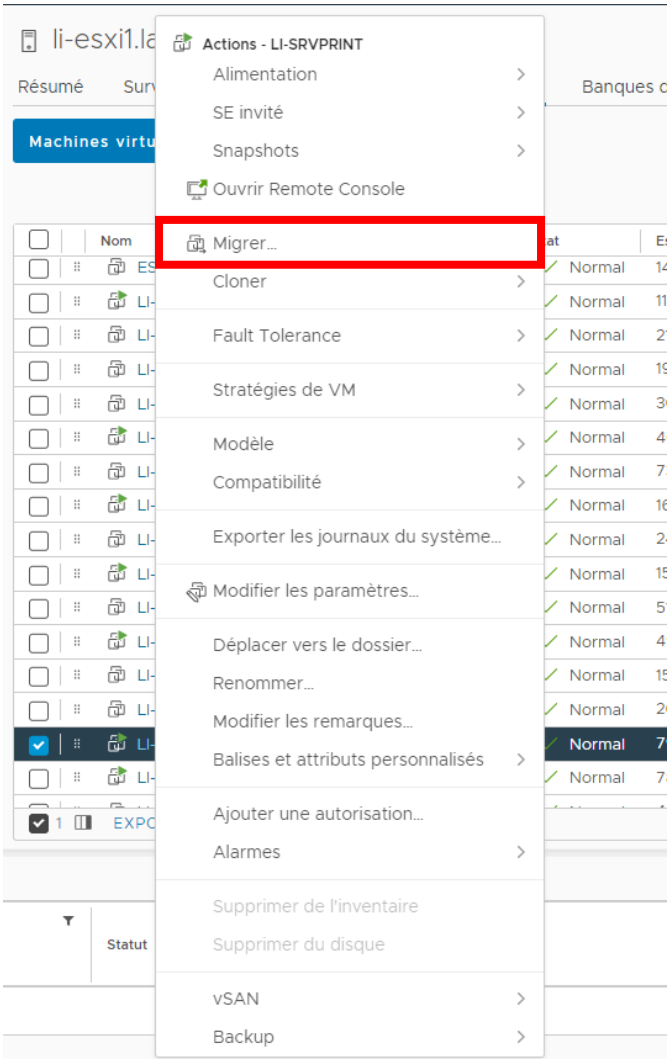
Gestion des VM critiques (comme Veeam)

L'une des étapes importantes concerne la gestion du serveur **Veeam**, une solution de sauvegarde. Si ce serveur est virtualisé, il est important de l'éteindre avant toute migration pour éviter tout problème de perte de données. Si Veeam est installé sur une machine physique, je m'assure de mettre à jour l'interface **iDRAC** (le contrôleur à distance de DELL) pour que tout soit à jour.

Dans le cas où le serveur est isolé, je créer également des règles temporaires pour prendre la main depuis le serveur de domaine (**DC**) et j'effectue la migration du serveur Veeam sans interruption. Une fois cette étape terminée, j'enlève la règle et reprends la main normalement.

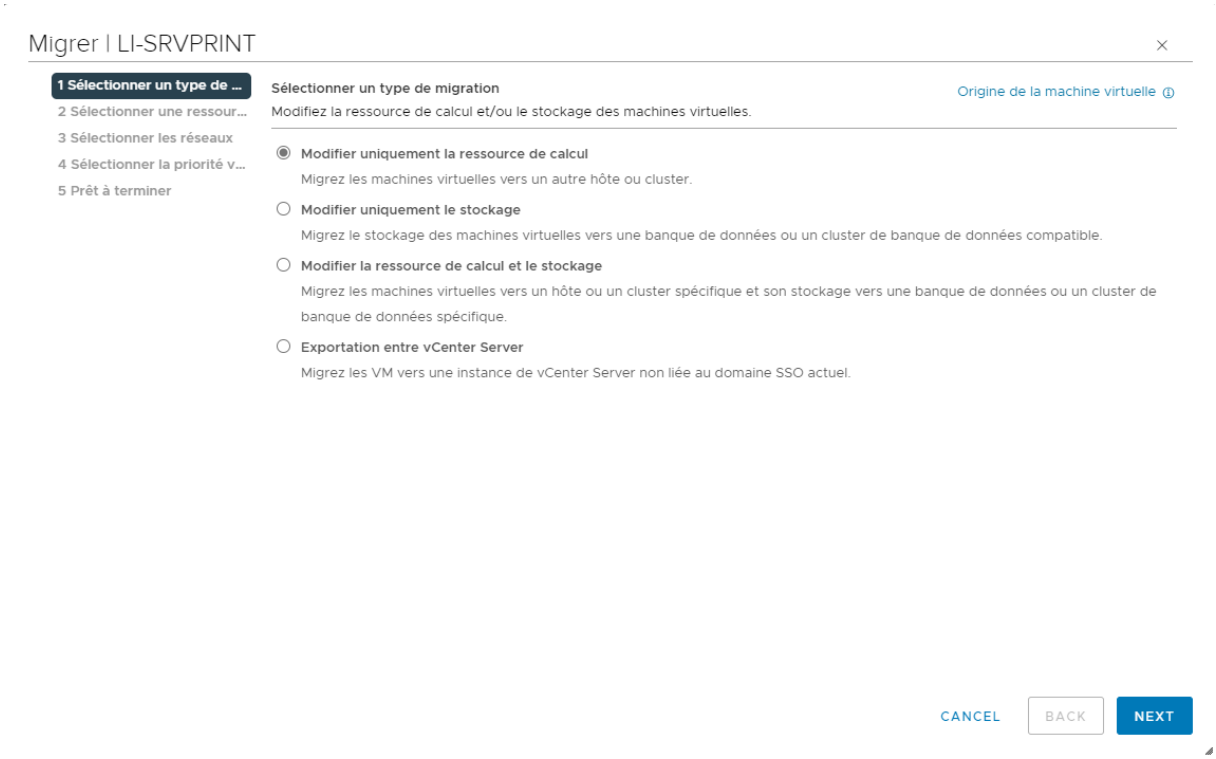
Migration des VM sur les hôtes ESXi

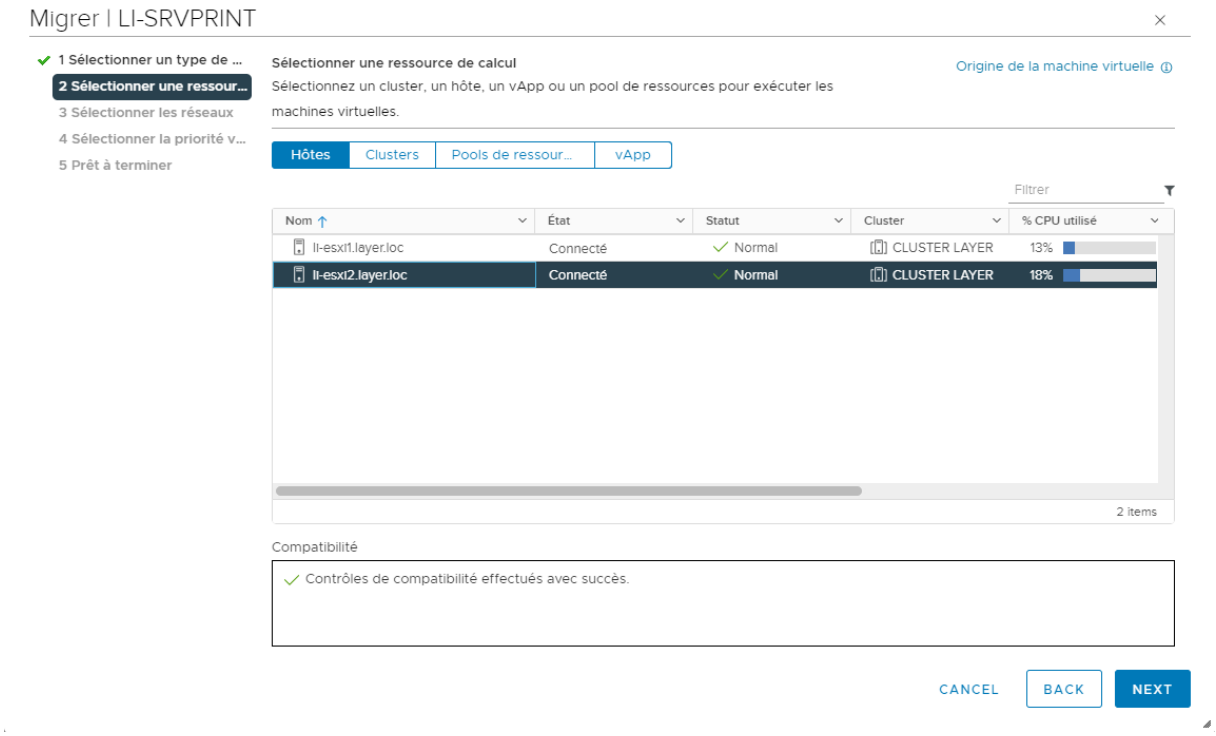
Je me concentre ensuite sur les **ESXi**. Pour chaque ESXi, je commence par lister les VM qui sont en marche. En fonction de l'infrastructure de stockage, je choisis l'option adaptée :

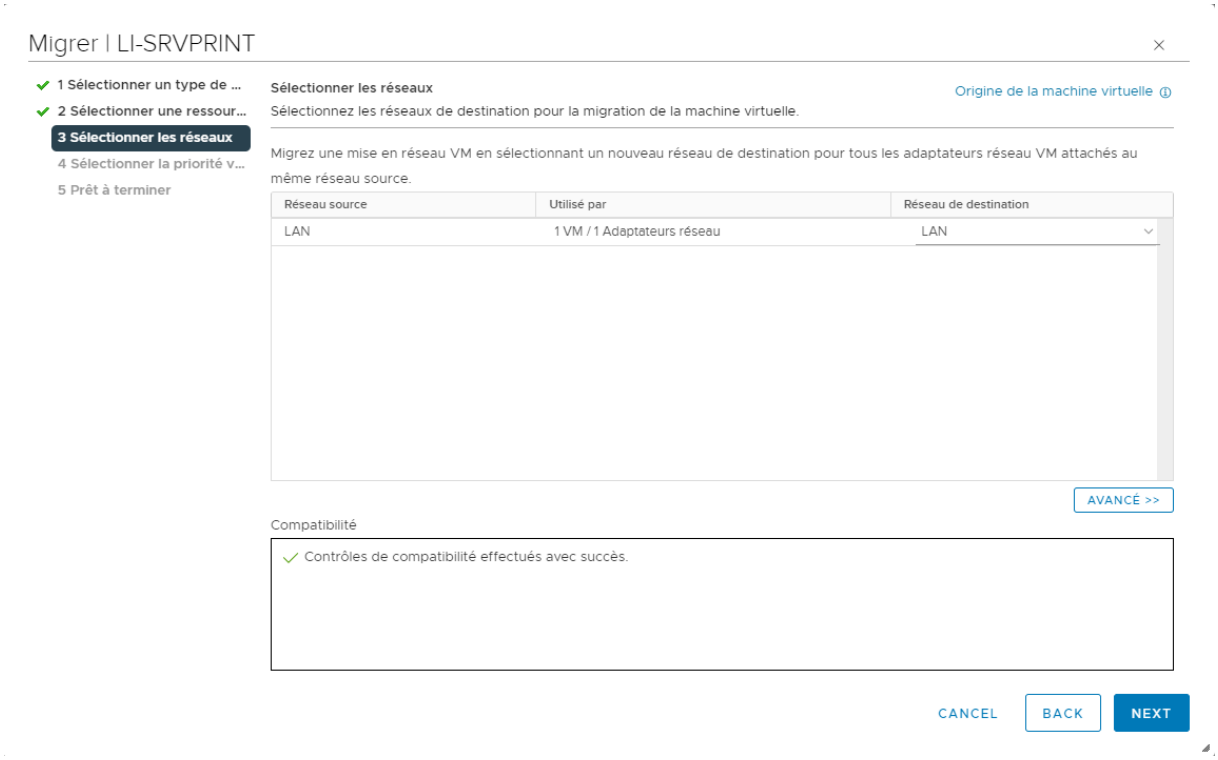


- Si un **SAN** (Stockage réseau) est disponible, je migre seulement les ressources de calcul des VMs d'un hôte à l'autre.

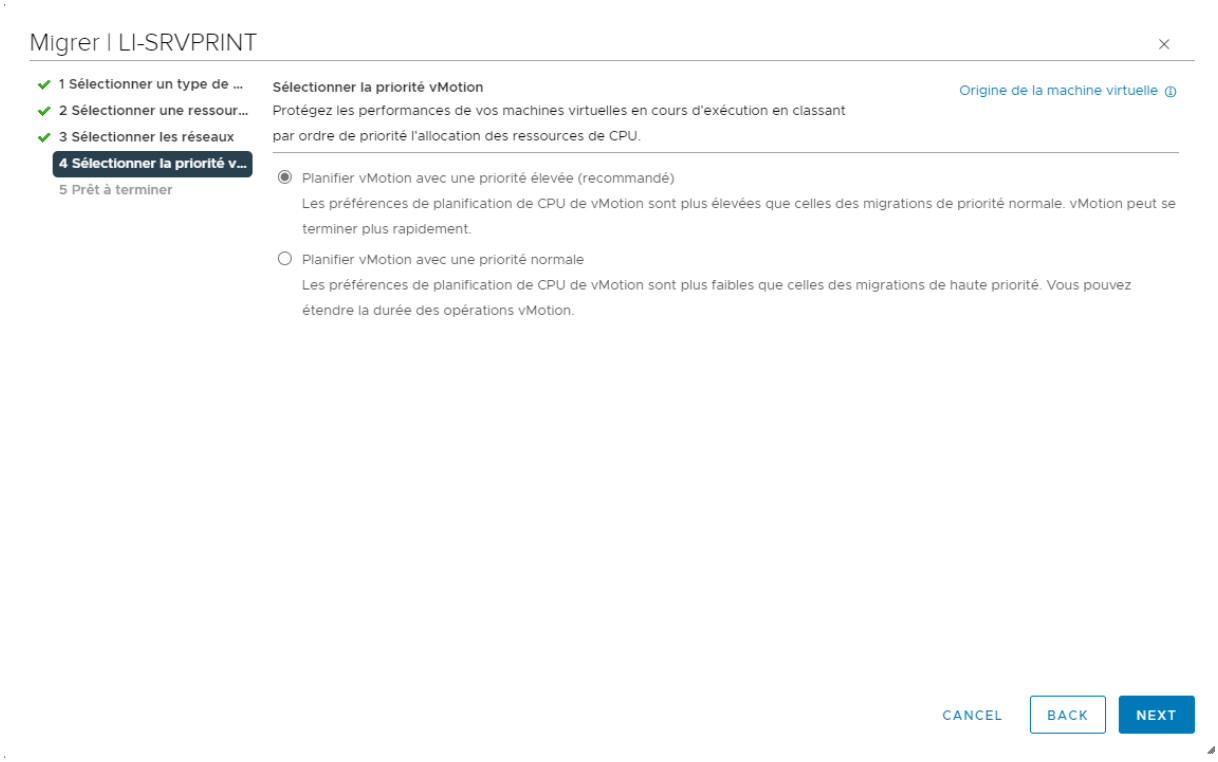
- Si aucun SAN n'est présent, je migre les calculs de ressources et le stockage en même temps.







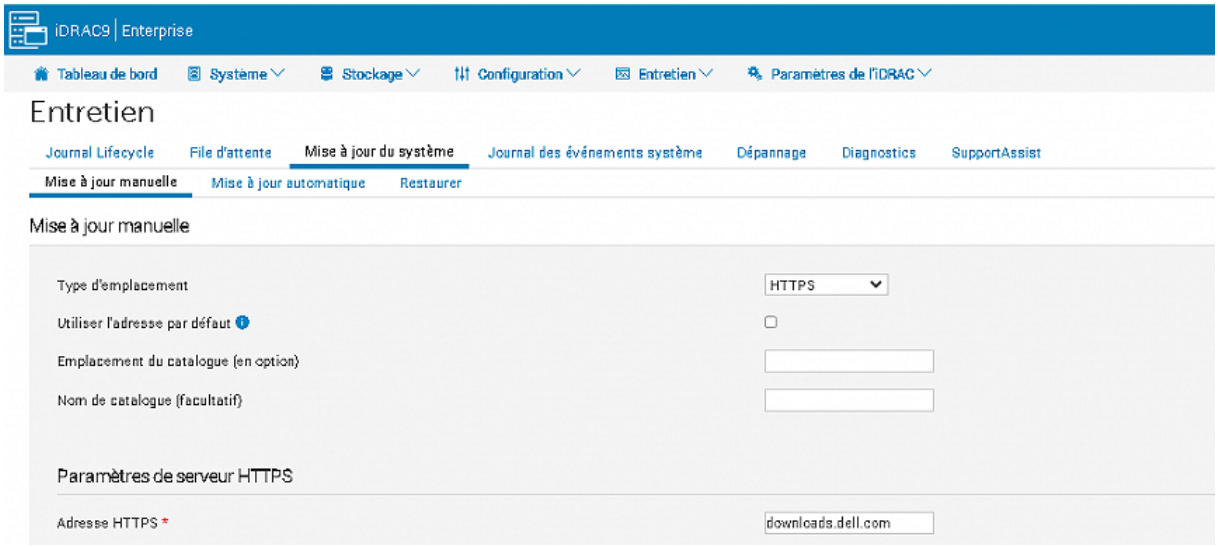
Pour chaque migration, je définis une **priorité élevée** afin de réduire au maximum le temps d'arrêt et je transfère les VMs d'un **ESXi 1 à ESXi 2**.



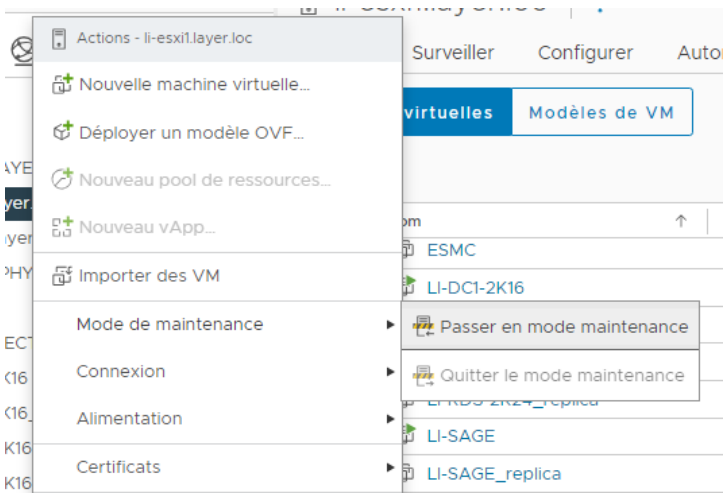
Mise à jour des hôtes ESXi et de l'iDRAC

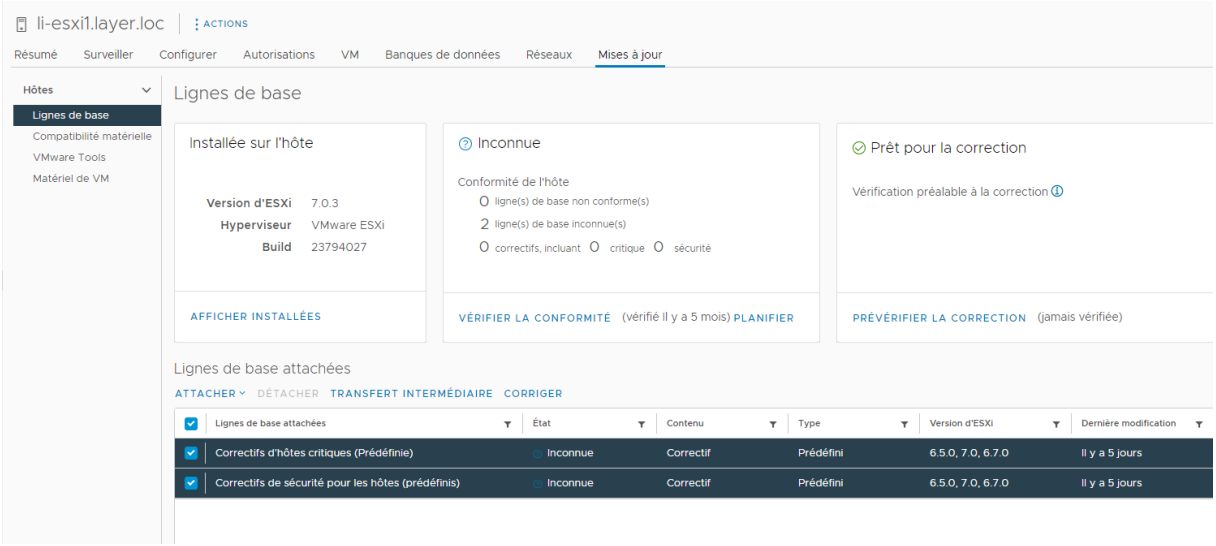
Une fois toutes les VM migrées, je passe à la mise à jour des hôtes **ESXi**. Mais avant cela, je dois m'assurer que l'interface de gestion à distance **iDRAC** est à jour. Cela me permet d'avoir un contrôle total à distance sur les serveurs en cas de problème.

Je me connecte à l'interface **iDRAC**, je vais dans l'onglet **Entretien > Mise à jour système** et je choisis de faire la mise à jour via **HTTPS** en utilisant l'adresse `downloads.dell.com`. Cette étape est cruciale car l'iDRAC me permet de redémarrer et de surveiller les serveurs sans devoir être physiquement présent.



Une fois l'iDRAC à jour, je mets l'**ESXi en mode maintenance** pour éviter tout problème. Je lance la mise à jour via l'onglet **Mise à jour**, où je sélectionne les correctifs de sécurité et les correctifs d'hôte. Après l'application des mises à jour, je vérifie que tout est conforme avant de réactiver les VMs sur l'hôte mis à jour.





Problèmes rencontrés durant les mises à jour

1. Isolement du réseau de gestion :

J'ai rencontré des problèmes avec les cartes réseaux pour le management qui sont gérées dans un sous-réseau isolé, ce qui a empêché les serveurs de se connecter aux serveurs de mise à jour via HTTPS. Pour résoudre ce problème, il a fallu télécharger manuellement l'ISO des mises à jour et effectuer les mises à jour par SSH.

Exemple de commande SSH :

- *esxcli system maintenanceMode set --enable=true*
- *esxcli software vib update --depot /vmfs/volumes/datastore/ISO/VMware-ESXi-7.0U3j-21053776-depot.zip*

2. Problèmes avec les VIB sur les serveurs ESXi :

J'ai également eu des difficultés avec certains **VIB** (Vib drivers) sur les serveurs ESXi, notamment les VIB **OpenManage** : **QEDF** et **QEDI**. Leur suppression était nécessaire pour éviter des conflits, mais cela a soulevé des questions concernant la stabilité et la fonctionnalité des systèmes post-suppression, en particulier pour les connexions de stockage. Étant donné qu'ils n'étaient pas utilisés, nous avons pu les supprimer sans problème.

Lien :

Procédure pour supprimer des VIB d'un hôte : Supprimer des VIB d'un hôte (vmware.com)

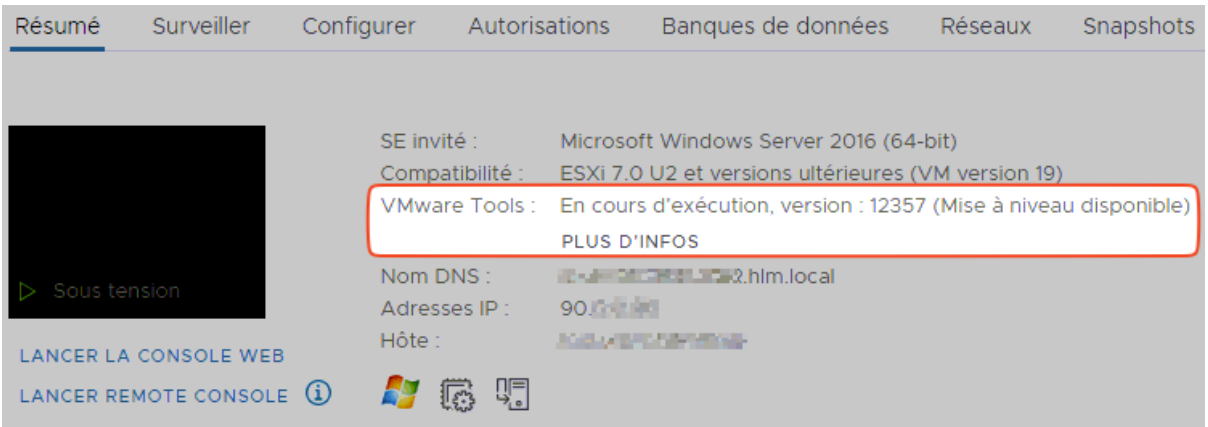
Mise à jour du vCenter

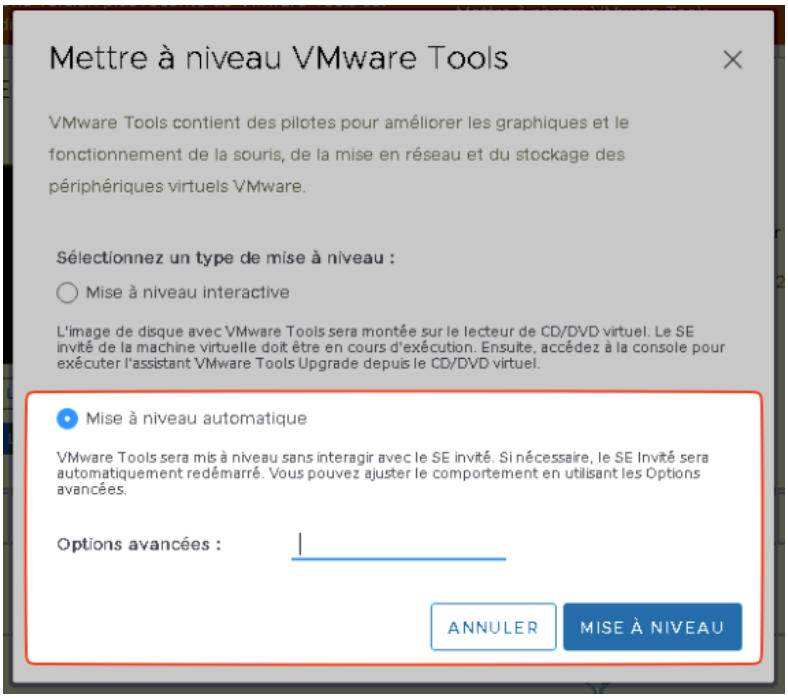
Une fois tous les ESXi à jour, je passe à la mise à jour du **vCenter**. Pour cela, je prends d'abord un **snapshot** de l'état actuel du vCenter (que je nomme **Avant MAJ VCSA**), au cas où il y aurait un problème durant la mise à jour.

Je me connecte ensuite au vCenter via le port **5480** et je vais dans l'onglet **Update**. Je lance l'option **Stage and Install**, j'accepte les conditions, et je coche l'option pour sauvegarder la base de données. Il est crucial de ne jamais redémarrer manuellement le vCenter pendant cette phase, car cela pourrait interrompre le processus de mise à jour.

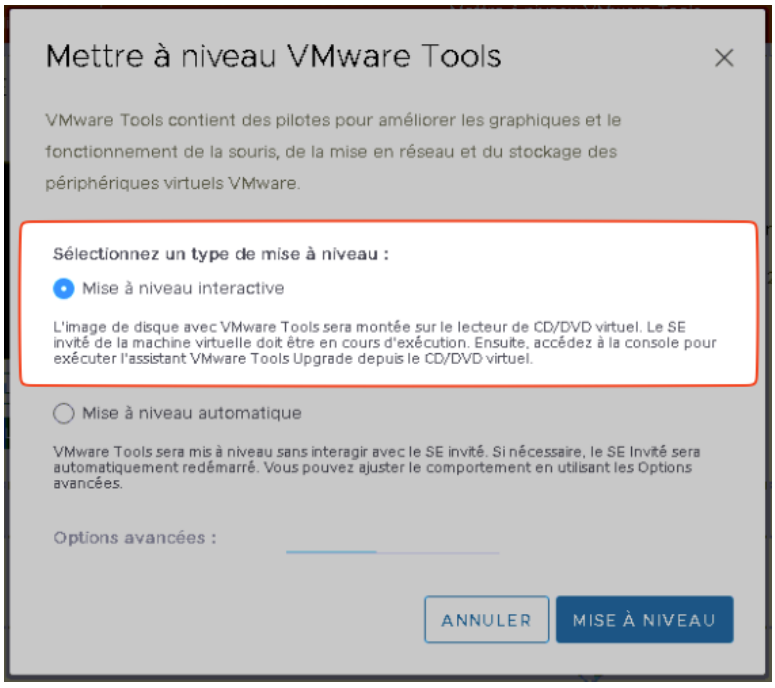
Mise à jour des VMware Tools

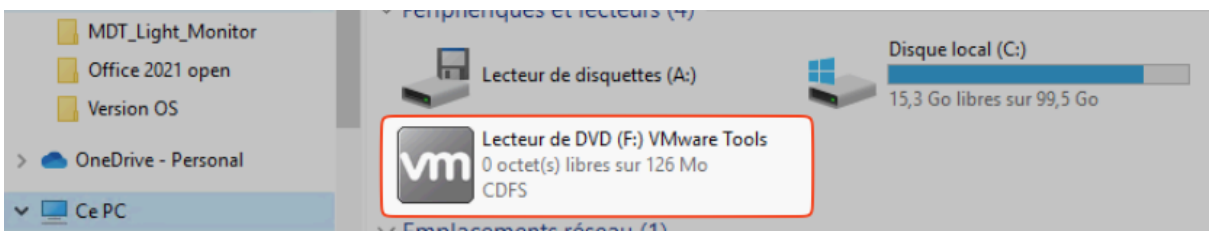
Enfin, après avoir mis à jour le vCenter et les ESXi, je mets à jour les **VMware Tools** sur les machines virtuelles tournant sous **Windows 10** ou **Windows Server 2016/2019/2022**. Si un redémarrage est nécessaire, je planifie cela avec les utilisateurs et je fais le redémarrage en dehors des heures de travail.





Si la mise à jour automatique des VMware Tools échoue, je passe en mode **Interactive** et je lance l'installation manuellement depuis un CD virtuel.





Création de procédure pour la mise à jour des VMware Tools

Pour répondre aux besoins de certains clients et confrères informaticiens qui souhaitaient gérer eux-mêmes les mises à jour des **VMware Tools**, j'ai élaboré une procédure simple et claire. Cette procédure décrit les étapes à suivre pour effectuer les mises à jour, assurant ainsi un transfert de compétences efficace et garantissant que les mises à jour soient réalisées correctement et sans problème.

Compétences acquises : transfert de compétences

Cette expérience m'a permis de développer mes compétences en documentation technique et en communication, en apprenant à créer des guides compréhensibles qui facilitent la transmission de connaissances à d'autres utilisateurs.

Nettoyage après les mises à jour

Après avoir terminé toutes les mises à jour, je prends le temps de tout remettre au propre. Cela inclut :

- La suppression des **licences temporaires** ajoutées en début de procédure.

- La suppression des **règles temporaires de pare-feu**.

- La suppression du **snapshot du vCenter** pris avant la mise à jour.

- La vérification et la remise en place du **démarrage automatique des VMs** sur les hôtes ESXi.

Partie 2 – Validation

Validation de la Protection et de la fonctionnalité pour le Client

Après l'achèvement des mises à jour et des opérations de maintenance, une série de validations a été effectuée pour garantir la sécurité et la fonctionnalité de l'infrastructure client :

1. **Validation client et documentation des interventions :**
   Le client a été informé du succès des opérations, et un rapport détaillant chaque étape de mise à jour a été fourni. Une documentation supplémentaire a été remise aux équipes internes ou clients, garantissant ainsi leur autonomie et la pérennité des changements appliqués.

2. **Vérification des mises à jour de sécurité :**
   Toutes les versions logicielles (ESXi, vCenter, VMware Tools) ont été vérifiées pour s'assurer qu'elles intègrent les derniers correctifs de sécurité fournis par VMware. Cela protège les clients contre les vulnérabilités connues et renforce la résilience de leur infrastructure IT.

Grâce à ces mises à jour et aux tests effectués, le client bénéficie désormais d'une infrastructure sécurisée, à jour, et entièrement fonctionnelle pour supporter leurs activités en toute tranquillité.

Ce que cette expérience m'a apporté

Cette expérience m'a permis d'approfondir mes compétences dans la gestion des infrastructures VMware, notamment en termes de gestion des licences, de migration de VM, et de maintenance des serveurs. J'ai appris à gérer les mises à jour complexes tout en assurant une continuité de service, ce qui est essentiel dans une infrastructure IT critique.

Partie 3 – Veille technologique

Veille Informatique

Nous consacrons du temps à l'étude approfondie des nouvelles failles de sécurité afin de maintenir nos clients à jour et de prévenir toute attaque potentielle sur leurs infrastructures. Cette veille continue est essentielle pour anticiper les risques et réagir rapidement aux menaces émergentes.

Il est important de noter que si certaines failles sont mineures et facilement corrigeables, d'autres peuvent s'avérer beaucoup plus critiques. Ces vulnérabilités majeures sont particulièrement dangereuses, car elles peuvent entraîner des perturbations graves, voire un arrêt complet de la production pour les clients. C'est pourquoi une surveillance rigoureuse et réactive est indispensable pour garantir la sécurité et la continuité des activités.

Outils et méthodes pour la veille informatique

Nous utilisons plusieurs moyens pour mettre en œuvre une veille informatique efficace et assurer la mise à jour des systèmes de nos clients. En tant que techniciens, nous avons un devoir de vigilance constante : identifier les failles de sécurité, les remonter rapidement et les traiter de manière proactive.

Pour cela, nous nous appuyons sur plusieurs ressources fiables :

1. Sites officiels :
   Nous consultons régulièrement des sites reconnus tels que Broadcom.com, Cybermalveillance.gouv.fr, et Sophos pour suivre les nouvelles vulnérabilités et obtenir des recommandations de sécurité officielles.
2. Forums spécialisés :
   Des plateformes comme IT-Connect nous permettent d'échanger avec d'autres professionnels, de partager des retours d'expérience et d'obtenir des conseils pratiques sur la gestion des failles.
3. Réseaux sociaux et veille personnelle :
   Nous utilisons également des réseaux comme Twitter pour obtenir des informations en temps réel. En suivant des experts de la cybersécurité ou des comptes institutionnels, nous pouvons repérer rapidement de nouvelles menaces. Il est cependant essentiel de vérifier la véracité des informations avant de remonter une faille et d'agir en conséquence.

Grâce à ces différentes sources, nous sommes en mesure de réagir rapidement et de garantir une sécurité optimale aux infrastructures de nos clients.