

République du Sénégal



Un peuple-Un but -Une Foi

Ministère de l'Enseignement Supérieur de la Recherche et de l'Innovation



GROUPE ISM

WINDOWS SERVER

L3 GLRS

A decorative blue scroll frame with a ribbon-like border, containing the title text.

VIRTUALISATION AVEC VMWARE ESXI

MODÉRATEURS :

Christ-David MONDJOT

Franck-ba Mabuila NKOUNGA

Alliance Trio Parfait MUNEZERO NIYTEGEKA

Kokou Godwin TCHAKPANA

PROFESSEUR :

M. Massamba LO

INTRODUCTION

Face à l'évolution rapide des technologies de l'information, les entreprises font face à des défis sans cesse croissants en matière de gestion des ressources informatiques. Un constat prédominant est celui de l'inefficacité dans l'utilisation des infrastructures matérielles, souvent caractérisée par une sous-utilisation des capacités des serveurs physiques, des coûts élevés de maintenance, et une complexité accrue de la gestion. C'est dans ce contexte que la virtualisation émerge comme une solution novatrice pour optimiser l'utilisation des ressources, simplifier la gestion, et accroître la flexibilité des infrastructures informatiques. La virtualisation fait face à ces défis en permettant la création de machines virtuelles, indépendantes du matériel sous-jacent, qui peuvent exécuter différents systèmes d'exploitation et applications. Cette approche offre une consolidation des ressources, une meilleure flexibilité pour adapter l'infrastructure aux besoins changeants, et une simplification notable de la gestion. En effet, en informatique, la virtualisation consiste à exécuter sur une machine hôte, dans un environnement isolé, des systèmes d'exploitation ou des applications. Ces ordinateurs virtuels sont appelés serveurs privés virtuels (Virtual Private Server ou VPS) ou environnements virtuels (Virtual Environment ou VE) ou encore machines virtuelles (VM). Un exemple symbolique de cette virtualisation est l'utilisation de solutions telles que VMware ESXi. Dans les lignes à suivre, nous allons présenter la virtualisation avec VMware ESXi, un hyperviseur de type 1.

I. DÉFINITION DES CONCEPTS

1. Virtualisation

La virtualisation est une technologie qui vous permet de créer plusieurs environnements simulés ou ressources dédiées à partir d'un seul système physique. Elle vise à optimiser l'utilisation des ressources matérielles en créant des instances virtuelles, également connues sous le nom de machines virtuelles (VM), qui fonctionnent de manière indépendante les unes des autres. Ces VM peuvent exécuter différents systèmes d'exploitation sur un seul serveur physique, ce qui améliore l'efficacité, la flexibilité, et la gestion des ressources. La virtualisation peut être appliquée à diverses couches de l'infrastructure informatique, y compris le calcul, le stockage, et le réseau.

2. Hyperviseur

Un hyperviseur ou encore gestionnaire de machines virtuelles est un logiciel qui permet la virtualisation des ressources informatiques. Il permet l'exécution simultanée de plusieurs systèmes d'exploitation sur une seule machine physique. Il est responsable de la gestion des ressources matérielles, telles que la mémoire et le stockage, et de la fourniture de machines virtuelles pour les systèmes d'exploitation et les applications. Il existe deux types d'hyperviseur :

- **Hyperviseurs de type 1 ou bare-metal** : il est installé directement sur le matériel. Il offre une performance optimale et une isolation complète entre les machines virtuelles. Il est principalement utilisé dans les environnements de serveurs.
- **Hyperviseurs de type 2 ou hébergé** : il s'exécute au-dessus d'un système d'exploitation hôte, ce qui peut introduire une certaine surcharge, mais il est plus flexible et adapté à un usage sur des postes de travail individuels.

3. VMware ESXi

VMware ESXi (*Elastic Sky X integrated*), développé par la société **VMware**, est l'une des solutions de virtualisation les plus populaires sur le marché. ESXi est un hyperviseur de type 1 développé par VMware pour le déploiement et la maintenance d'ordinateurs. Il s'installe directement sur le matériel physique, sans nécessiter de système d'exploitation hôte. Cela permet une gestion plus efficace des ressources et une performance optimale des machines virtuelles.

4. Hôte

Un hôte fait référence à la machine physique sur laquelle un hyperviseur de virtualisation est installé. Cet hôte, également appelé ‘*serveur hôte*’ ou ‘*host*’ en anglais, constitue la base sur laquelle des machines virtuelles peuvent être créées et exécutées.

5. Invité

Un invité se réfère à une machine virtuelle qui fonctionne à l'intérieur d'un environnement virtualisé sur un hôte physique. L'invité est une instance virtuelle d'un système d'exploitation qui peut être exécutée sur le matériel physique de l'hôte grâce à l'hyperviseur. Chaque invité a ses propres ressources virtuelles assignées, telles que la mémoire, le stockage, et les interfaces réseau, assurant ainsi une isolation entre différentes machines virtuelles.

II. QUELQUES INFORMATION SUR VMWARE ESXi

A. Qu'est-ce que VMware ESXi ?

VMware ESXi est un hyperviseur de type 1, également connu sous le nom de bare-metal hypervisor, développé par VMware. Il s'agit d'un logiciel qui s'installe directement sur le matériel physique d'un serveur et permet de virtualiser plusieurs systèmes d'exploitation sur une seule machine physique.

1) Historique et évolution

VMware ESXi a été introduit pour la première fois en 2001 sous le nom de VMware ESX Server. Il s'agissait d'un hyperviseur de type 2, ce qui signifie qu'il s'exécutait sur un système d'exploitation hôte.

En 2006, VMware a publié ESXi 3.0, le premier hyperviseur de type 1 de la société. ESXi 3.0 a été conçu pour s'exécuter directement sur le matériel, sans système d'exploitation hôte sous-jacent. Cela a permis d'améliorer les performances, la sécurité et la fiabilité.

Les versions ultérieures d'ESXi ont continué à ajouter de nouvelles fonctionnalités et améliorations, notamment avec les versions :

ESXi 4.0 (2009) : Prise en charge de la virtualisation matérielle, des machines virtuelles 64 bits et de vMotion pour la migration en direct des machines virtuelles.

ESXi 5.0 (2011) : Prise en charge de la haute disponibilité, du stockage partagé et de la gestion centralisée via vCenter Server.

ESXi 5.5 (2013) : Prise en charge des machines virtuelles imbriquées, du chiffrement des machines virtuelles et de la protection contre les logiciels malveillants.

ESXi 6.0 (2015) : Prise en charge des conteneurs Docker, des réseaux définis par logiciel (SDN) et de la gestion basée sur des stratégies.

ESXi 6.5 (2017) : Prise en charge des machines virtuelles avec mémoire persistante, de la sécurité basée sur le microprogramme et de l'automatisation des opérations.

ESXi 7.0 (2019) : Prise en charge des processeurs AMD EPYC, des machines virtuelles avec accélération matérielle et de la gestion des mises à jour du microprogramme.

ESXi 8.0 (2023) : Prise en charge des processeurs Intel Xeon Scalable de 4e génération, des machines virtuelles avec accélération GPU et des fonctionnalités de sécurité améliorées.

Aujourd'hui, VMware ESXi est l'un des hyperviseurs les plus populaires au monde, utilisé par les entreprises de toutes tailles pour virtualiser leurs charges de travail. Il est connu pour ses performances, sa fiabilité, sa sécurité et ses fonctionnalités de gestion complètes.

2) Caractéristiques clés de ESXi

VMware ESXi est un hyperviseur de type 1 bare-metal qui offre les fonctionnalités clés suivantes : **La Virtualisation matérielle**, ESXi prend en charge la virtualisation matérielle, ce qui permet aux machines virtuelles d'accéder directement aux ressources matérielles, telles que les processeurs, la mémoire et les périphériques d'E/S. De plus, ESXi **prend en charge les machines virtuelles 64 bits**, ce qui permet aux charges de travail d'accéder à de grandes quantités de mémoire et de bénéficier de meilleures performances. **Il dispose également d'une fonctionnalité appelée vMotion**, la vMotion est une fonctionnalité qui permet de migrer en direct des machines virtuelles en cours d'exécution d'un hôte ESXi vers un autre sans interruption de service. **La Haute disponibilité**, ESXi prend en charge la haute disponibilité, ce qui permet de créer des clusters de serveurs ESXi qui fournissent une redondance et une tolérance aux pannes. De même, **Stockage partagé**, ESXi prend en charge le stockage partagé, ce qui permet aux machines virtuelles de stocker leurs données sur un stockage partagé

accessible à tous les hôtes ESXi du cluster. De plus, **Gestion centralisée**, ESXi peut être géré de manière centralisée à l'aide de VMware VCenter Server, qui fournit une interface unique pour gérer plusieurs hôtes ESXi et machines virtuelles. **Les Conteneurs Docker**, ESXi prend en charge les conteneurs Docker, ce qui permet aux organisations de déployer et de gérer des applications conteneurisées dans des environnements virtualisés. De plus, **Réseaux définis par logiciel (SDN)**, ESXi prend en charge les SDN, ce qui permet aux administrateurs de créer et de gérer des réseaux virtuels de manière logicielle. En outre, **Gestion basée sur des stratégies**, ESXi prend en charge la gestion basée sur des stratégies, ce qui permet aux administrateurs de définir et d'appliquer des stratégies pour automatiser la gestion des machines virtuelles et des hôtes ESXi. **Les Machines virtuelles avec mémoire persistante**, ESXi prend en charge les machines virtuelles avec mémoire persistante, ce qui permet aux machines virtuelles d'accéder à des pools de mémoire plus grands et plus rapides. **la Sécurité basée sur le microprogramme**, ESXi intègre des fonctionnalités de sécurité basées sur le microprogramme, telles que Secure Boot et Trusted Platform Module (TPM), pour améliorer la sécurité de l'environnement virtualisé. **L'Automatisation des opérations**, ESXi prend en charge l'automatisation des opérations, ce qui permet aux administrateurs d'automatiser des tâches courantes telles que le provisionnement, la gestion et la mise à jour des machines virtuelles et des hôtes ESXi.

Ces fonctionnalités clés font de VMware ESXi une solution de virtualisation puissante et complète.

B. Avantages et Inconvénients de l'utilisation de VMware ESXi

1) Les avantages

VMware ESXi offre de nombreux avantages qui en font une solution de virtualisation populaire pour les entreprises.

- **Grace à la Consolidation du serveur** : ce qui Réduit le nombre de serveurs physiques nécessaires en virtualisant plusieurs charges de travail sur une seule machine.
- **L'Optimisation des ressources** : elle Alloue dynamiquement les ressources matérielles aux machines virtuelles, améliorant l'utilisation du matériel.
- **Haute disponibilité** : Assure la disponibilité continue des applications en cas de panne matérielle ou logicielle.
- **Gestion simplifiée** : Fournit une console centralisée pour gérer plusieurs hôtes et machines virtuelles, simplifiant les opérations.

- **Sécurité accrue** : Isolement des machines virtuelles et des fonctionnalités de sécurité intégrées améliorent la sécurité globale.

2) Les inconvénients

Malgré ses nombreux avantages, VMware ESXi présente également quelques inconvénients à prendre en compte :

- En premier lieu **le Coût** : VMware ESXi est un logiciel propriétaire et nécessite une licence pour son utilisation. Les coûts de licence peuvent être élevés, surtout pour les environnements à grande échelle.
- **La Complexité** : La configuration et la gestion d'ESXi peuvent être complexes, surtout pour les administrateurs novices. Une expertise et des connaissances approfondies sont nécessaires pour optimiser les performances et la sécurité.
- **La Dépendance au matériel** : ESXi est étroitement lié au matériel sur lequel il s'exécute. Les mises à niveau ou les modifications matérielles peuvent nécessiter une réinstallation ou une reconfiguration d'ESXi.
- **Le Verrouillage du fournisseur** : L'utilisation d'ESXi peut entraîner un verrouillage du fournisseur, car les machines virtuelles créées sur ESXi ne sont pas facilement portables vers d'autres hyperviseurs.
- **Les Performances** : Bien que ESXi offre de bonnes performances, il peut y avoir une légère surcharge par rapport à l'exécution de machines virtuelles directement sur du matériel physique.
- **Les Besoins en stockage** : Les machines virtuelles nécessitent un espace de stockage important, ce qui peut entraîner des coûts supplémentaires pour l'achat et la gestion du stockage.
- Enfin **la Sécurité** : Bien que ESXi intègre des fonctionnalités de sécurité, il est toujours essentiel de mettre en œuvre des mesures de sécurité supplémentaires, telles que les pare-feux et les logiciels antivirus, pour protéger l'environnement virtualisé.

C. Sécurité dans VMware ESXi

Garantir l'intégrité, la confidentialité et la disponibilité des infrastructures virtualisées est de la plus haute importance en matière de sécurité dans VMware ESXi. L'authentification et le contrôle d'accès, ainsi que l'isolation des machines virtuelles, sont les deux composants clés qui

constituent le cadre de sécurité de VMware ESXi. L'architecture de l'hyperviseur ESXi intègre de nombreuses fonctionnalités de sécurité, telles que l'isolation du CPU, l'isolation de la mémoire et l'isolation des périphériques.

1. Authentification et contrôle d'accès

VMware ESXi assure une sécurité robuste par le biais de mécanismes d'authentification avancés et de contrôle d'accès. Les administrateurs peuvent mettre en œuvre des politiques d'authentification robustes telles que l'authentification multifactorielle, la gestion des certificats, et l'intégration avec des services d'annuaire tels que LDAP ou Active Directory. Ces mesures renforcent l'identification des utilisateurs et garantissent un accès sécurisé au système ESXi.

En outre, VMware ESXi propose des fonctionnalités de contrôle d'accès granulaire, permettant aux administrateurs de définir des permissions spécifiques pour les utilisateurs et les équipes, restreignant ainsi l'accès à certaines fonctions ou machines virtuelles. Ceci contribue à limiter les risques d'accès non autorisés et à renforcer la confidentialité des données.

2. Isolation des machines virtuelles

L'isolation des machines virtuelles constitue une composante essentielle de la sécurité dans VMware ESXi. Chaque machine virtuelle fonctionne de manière indépendante, bénéficiant d'une séparation totale au niveau des ressources matérielles et des fichiers système. Cette isolation empêche la propagation de vulnérabilités potentielles d'une machine virtuelle à une autre, renforçant ainsi la résilience du système global.

De plus, VMware ESXi propose des fonctionnalités telles que la segmentation de réseau virtuel, permettant de créer des réseaux isolés pour les machines virtuelles sensibles, renforçant ainsi la sécurité des communications entre elles.

3. Sécurité des communications

La sécurité des communications dans VMware ESXi repose sur plusieurs mécanismes visant à garantir la confidentialité, l'intégrité et l'authenticité des données transitant au sein de l'environnement virtualisé. L'utilisation de protocoles de chiffrement tels que SSL/TLS assure un niveau élevé de confidentialité en cryptant les données pendant leur transit. Cette couche de sécurité s'étend aux interactions entre les différents composants d'ESXi, tels que les connexions entre les administrateurs et la console de gestion, ou les échanges entre les machines virtuelles.

Parallèlement, des contrôles d'intégrité sont mis en place pour garantir que les données ne sont pas altérées pendant le transfert. Ces mécanismes vérifient l'intégrité des paquets de données pour détecter toute altération ou tentative de manipulation. Ainsi, la sécurité des communications dans VMware ESXi assure un environnement où les échanges d'informations sont protégés contre les interceptions non autorisées et les altérations malveillantes.

4. Gestion des certificats

La gestion des certificats dans VMware ESXi constitue un élément clé de la sécurité, assurant l'authenticité des composants et des communications au sein de l'environnement virtualisé. Les certificats SSL/TLS sont utilisés pour établir des connexions sécurisées, authentifier les serveurs ESXi et garantir que les utilisateurs interagissent avec des instances légitimes.

Une gestion proactive des certificats inclut des politiques de renouvellement régulier pour éviter les problèmes liés à l'expiration des certificats. Les administrateurs peuvent configurer des notifications pour être informés des éventuels problèmes de certificats, permettant ainsi une intervention rapide en cas de besoin. En outre, la possibilité de déployer des certificats signés par une autorité de certification renforce la confiance dans l'authenticité des connexions et contribue à la sécurité globale de l'environnement.

III. SOLUTION : INSTALLATION DE VMware ESXI

A. Prérequis pour l'installation

Avant de débiter l'installation de VMware ESXi, il est crucial de s'assurer que notre système réponde aux exigences minimales. Voici les prérequis typiques :

- **Processeur 64 bits avec virtualisation matérielle activée** : S'assurer que notre processeur supporte les extensions de virtualisation comme Intel VT-x ou AMD-V.
- **Au moins 4 Go de RAM** : Une quantité suffisante de mémoire vive pour garantir les performances de la virtualisation.
- **Espace de stockage** : Un disque dur d'au moins 32 Go d'espace disponible pour l'installation d'ESXi.
- **Carte réseau compatible** : Une carte réseau compatible est nécessaire pour assurer la connectivité réseau (Consulter le site officiel de VMware pour plus d'informations).

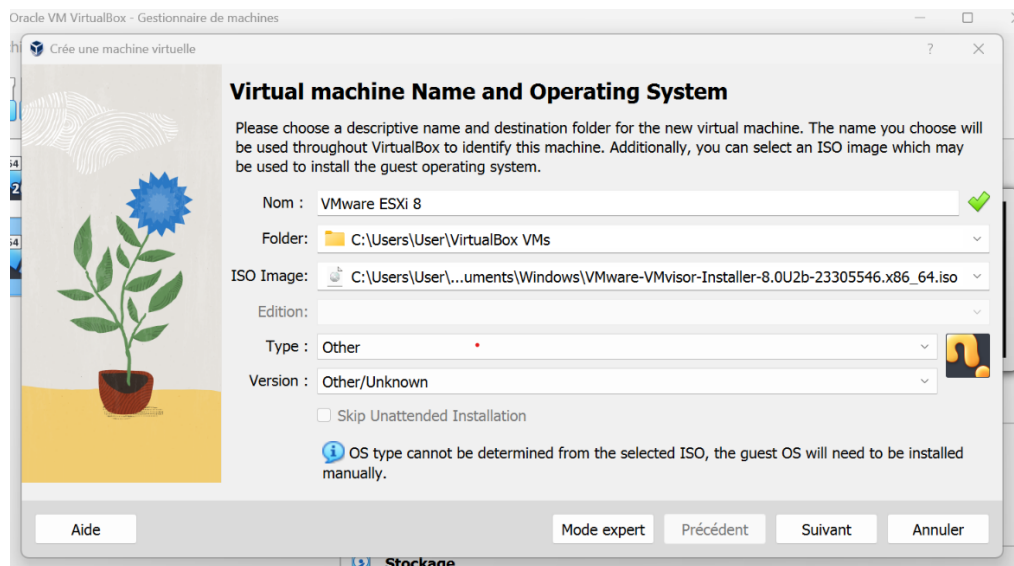
Puis, consulter la liste de compatibilité matérielle fournie par VMware pour garantir que notre matériel est pris en charge par la version spécifique d'ESXi que nous prévoyons d'installer. Cela peut être vérifié sur le site web officiel de VMware.

B. Processus d'installation de VMware ESXi

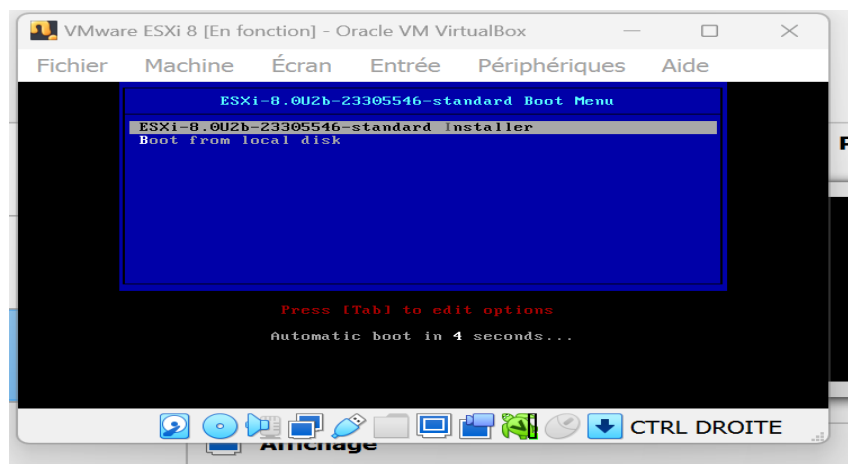
Dans ce cas précis, nous allons simuler l'installation de VMware ESXi 8.0.2 sur VMware Workstation Pro plutôt que sur notre machine physique car cette dernière est présente pas les prérequis.

[1] Télécharger VMWare ESXi 8.0.2 sous format iso directement sur le site officiel de VMware.

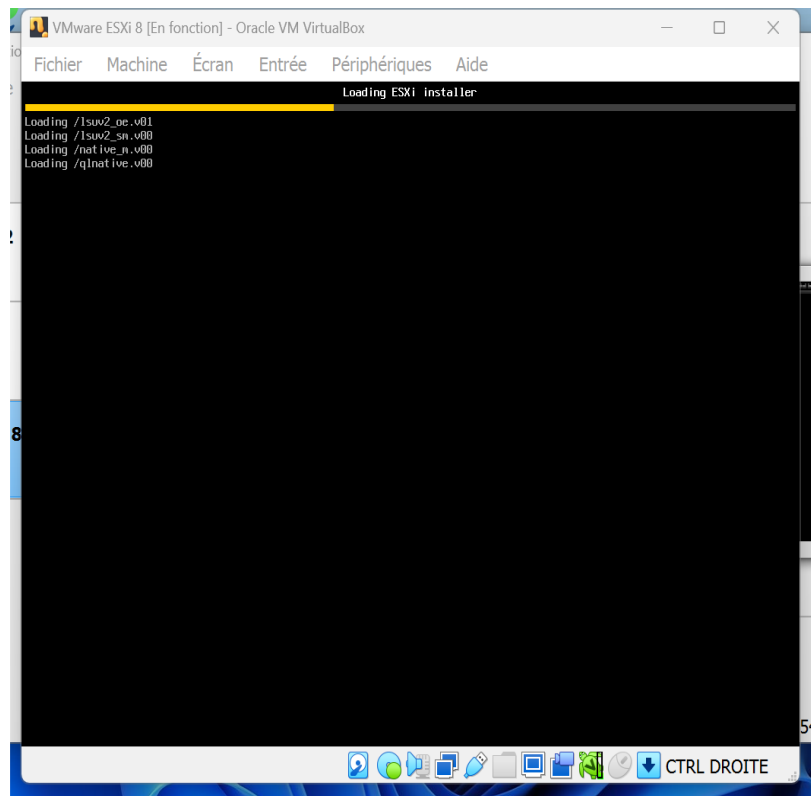
[2] Créer une machine virtuelle d'au moins 4Go RAM et 50Go Stockage à partir du fichier iso



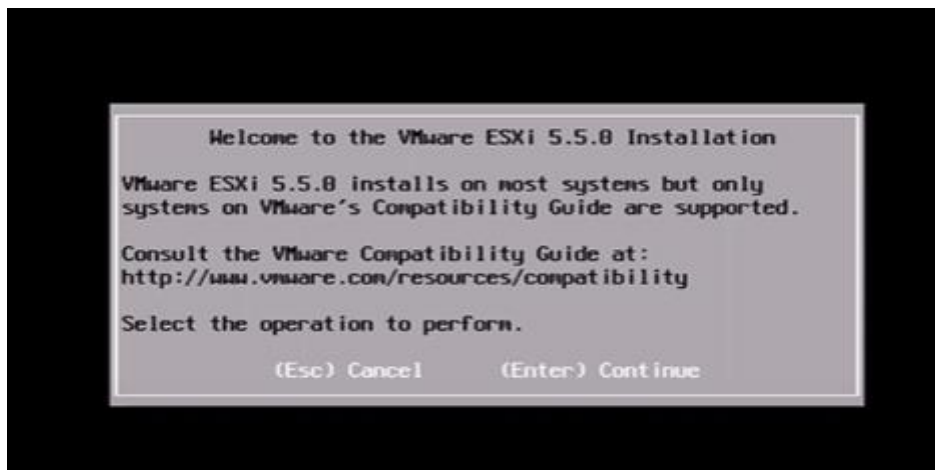
[3] Lancer la machine virtuelle et patienter. Choisir la première option ;

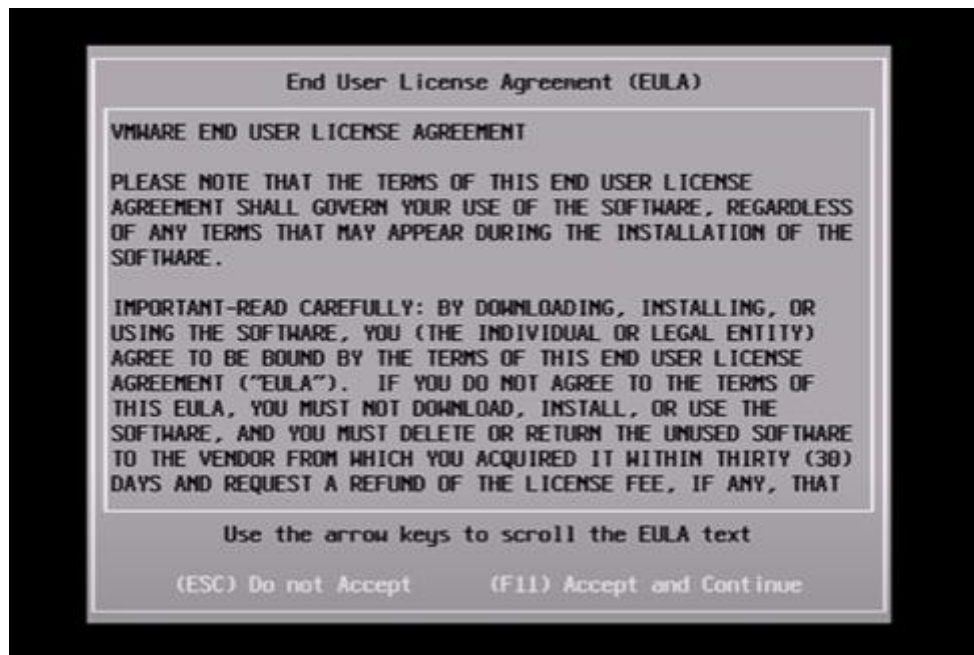


[4] Patienter la vérification des prérequis



[5] Accepter les termes et conditions d'utilisation, puis continuer ;





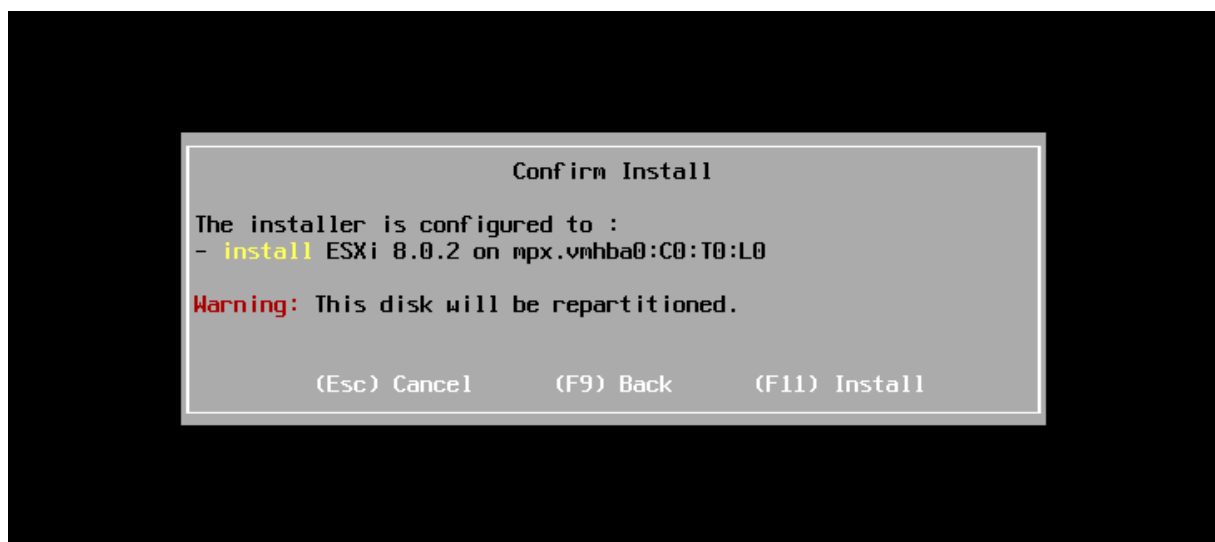
[6] Choisir la langue du clavier ;



[7] Choisir le mot de passe de l'administrateur : le mot de passe doit contenir au moins une majuscule, un caractère spécial et un chiffre ; Puis taper sur la touche ENTRER



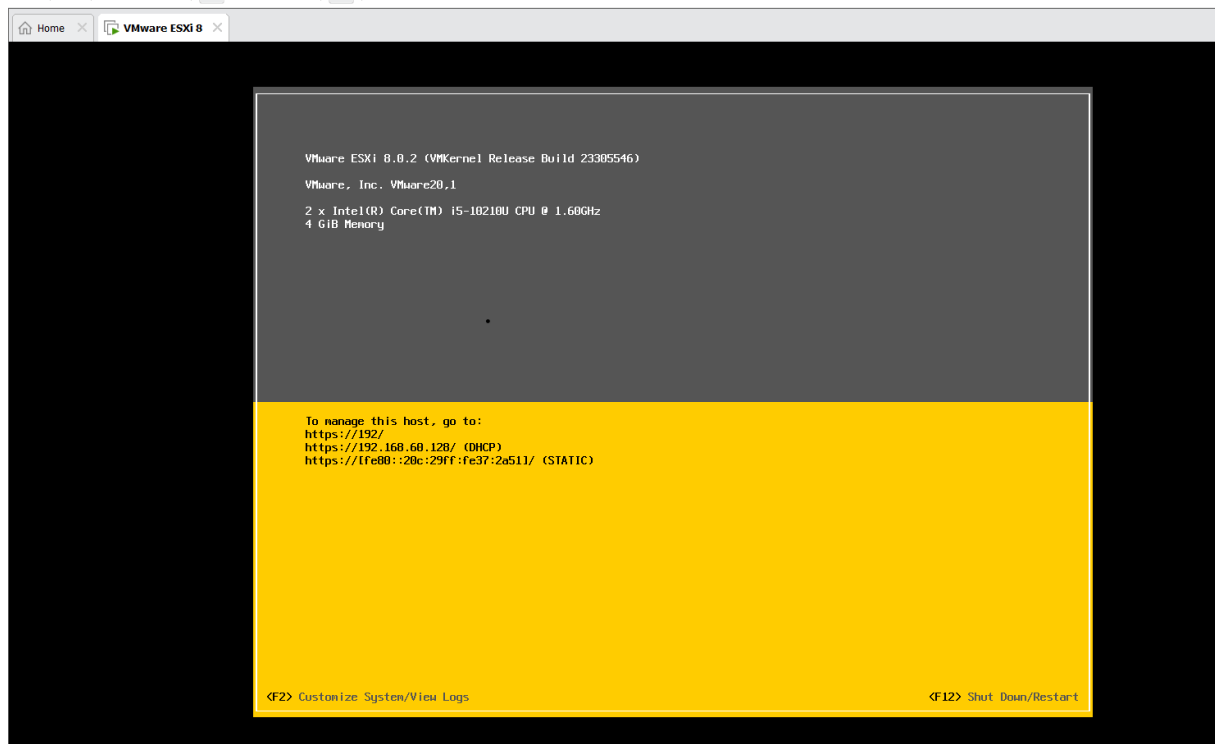
[8] Lancer l'installation à partir de la touche de fonction F11 et patienter le temps que l'installation finisse ;



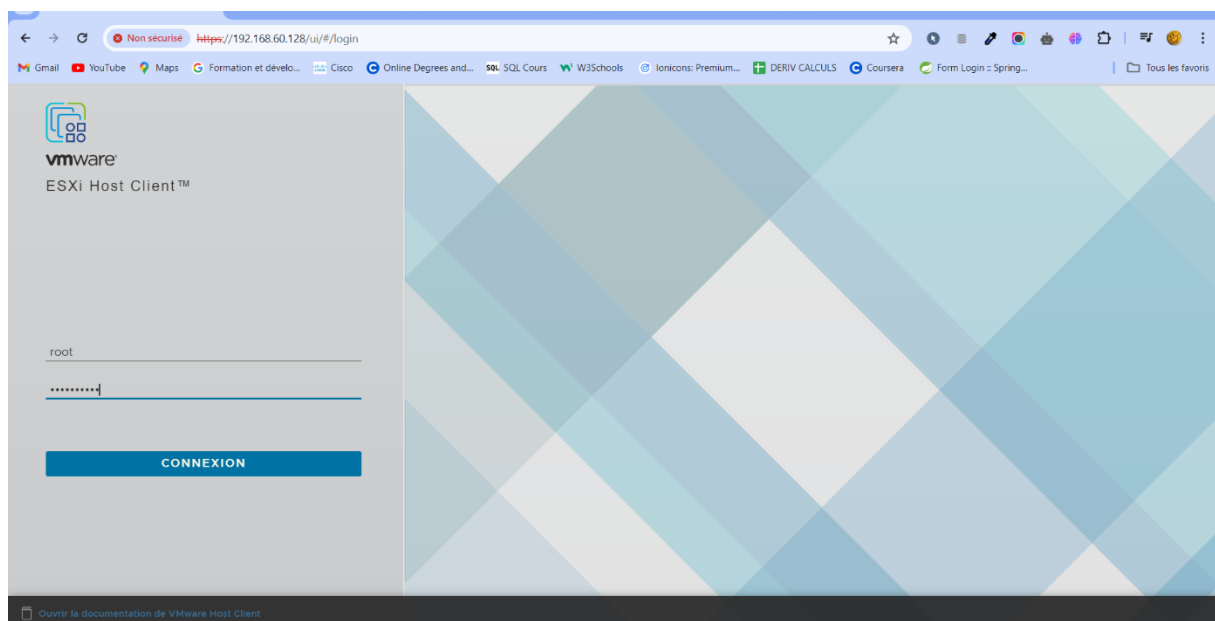
[9] Une fois l'installation finie, taper sur ENTRER pour redémarrer ;



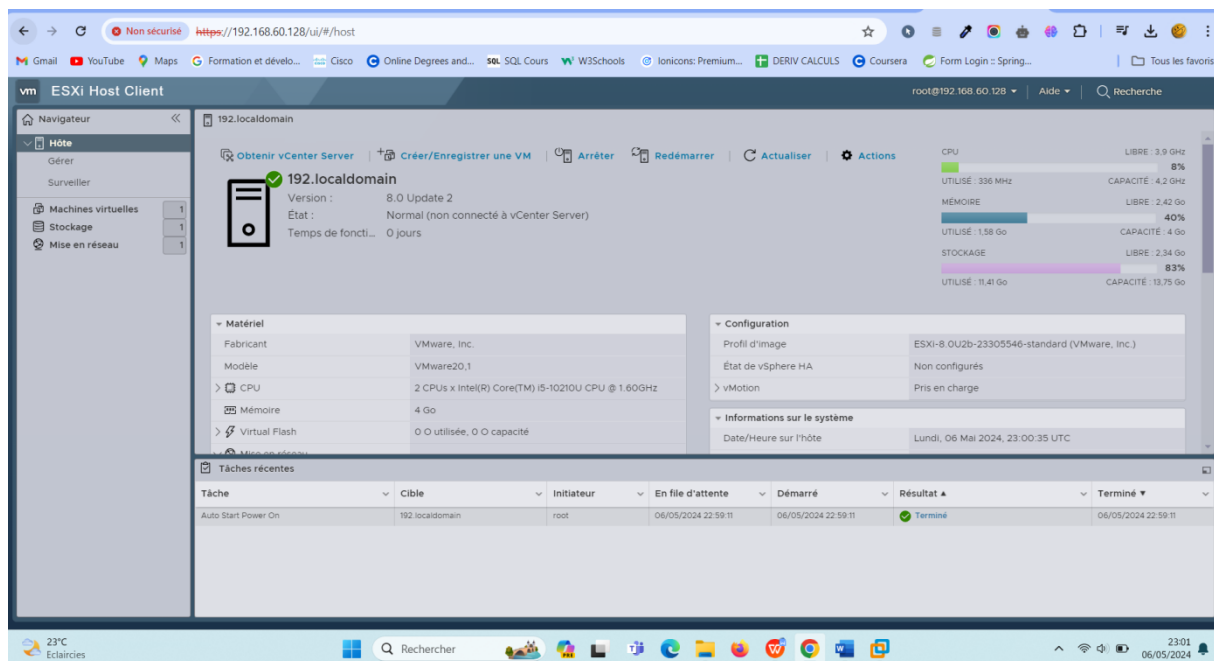
[9] Arriver ici, l'installation est terminée et on peut accéder à l'interface client en tapant l'url fourni dans un navigateur. Ici : <https://192.168.60.128>



[10] Voici le client du ESXI, il faut se connecter avec nos identifiants. Par défaut l'utilisateur est root et le mot de passe est celui saisi au moment de l'installation (Prendre en compte la disposition du clavier choisie lors de l'installation et celle de notre machine physique).



[11] Voici le client du VMware ESXi :



IV. LES APPLICATION DE VMware ESXi

- **Consolidation de serveurs**

VMware ESXi permet de consolider plusieurs serveurs physiques en une seule machine physique. Cela signifie qu'un seul serveur peut exécuter plusieurs machines virtuelles, ce qui permet d'optimiser l'utilisation des ressources matérielles et de réduire les coûts liés à l'infrastructure informatique.

- **Laboratoires de test et de développement**

Les environnements de test et de développement peuvent être créés rapidement et facilement en utilisant des machines virtuelles sur VMware ESXi. Cela permet aux développeurs de tester de nouvelles applications et configurations sans affecter l'environnement de production

- **Serveurs de production**

VMware ESXi est souvent déployé sur des serveurs de production pour exécuter des applications et des services essentiels à l'activité de l'entreprise. Les machines virtuelles créées sur VMware ESXi peuvent héberger divers services tels que des bases de données,

des serveurs de fichiers, des applications métier, des serveurs web, etc. La capacité de VMware ESXi à isoler les applications dans des machines virtuelles distinctes garantit une sécurité et une fiabilité accrues pour les services hébergés.

- **Services cloud**

De nombreuses entreprises utilisent VMware ESXi pour créer des environnements de cloud privé. En déployant VMware ESXi sur des serveurs dédiés, les entreprises peuvent offrir des services cloud internes à leurs utilisateurs, en leur permettant de provisionner rapidement des machines virtuelles pour leurs besoins de développement, de test ou de production. VMware propose également des solutions de cloud hybride et de cloud public basées sur sa technologie de virtualisation.

CONCLUSION

En conclusion, VMware ESXi se distingue comme une solution de virtualisation de premier plan, offrant des avantages significatifs pour l'efficacité opérationnelle et la gestion des ressources informatiques. En adoptant un modèle d'hyperviseur de type 1, ESXi permet une utilisation optimale des serveurs physiques en créant et en gérant efficacement des machines virtuelles. Les fonctionnalités avancées telles que la migration à chaud, la gestion centralisée via vCenter Server, la sécurité renforcée, et la prise en charge de divers systèmes d'exploitation invités, font de VMware ESXi un choix privilégié pour les entreprises cherchant à consolider leurs infrastructures, à améliorer la flexibilité des charges de travail, et à simplifier la gestion des environnements virtualisés. En tant que pilier de la virtualisation, VMware ESXi continue de jouer un rôle crucial dans l'évolution des infrastructures informatiques, offrant une base solide pour répondre aux exigences changeantes du paysage technologique actuel.