**RAPPORT 1 :**

**INITIATION A L’INFONUAGIQUE**



**SOUS-thème :**

**Virtualisation et configuration**

**Présenter par :**

**NDONG MBA VALENTINO**

**PLAN :**

**INTRODUCTION**

**Définition et Schématisation**

**Développement**

**Configuration**

**Firewall et sécurité**

**-utilisateurs et groups**

**-Ajouts (réseaux,disque,ports)**

**-alarmes**

**-customs**

**INTRODUCTION :**

**Définition et Schématisation**



La virtualisation consiste à **créer une représentation virtuelle, basée logicielle, d’un objet ou d’une ressource** telle qu’un système d’exploitation, un serveur, un système de stockage ou un réseau. Ces ressources simulées ou émulées sont en tous points identiques à leur version physique.



Les **machines virtuelles sont exécutées sur une couche d’abstraction matérielle**. Ainsi, les entreprises sont en mesure d’exécuter plusieurs systèmes d’exploitation et applications simultanément sur un serveur unique. Les ressources et capacités du serveur sont réparties entre les différentes instances. Ceci permet de réaliser d’importantes économies et d’utiliser les serveurs plus efficacement puisque leurs capacités sont pleinement exploitées.

**Développement**

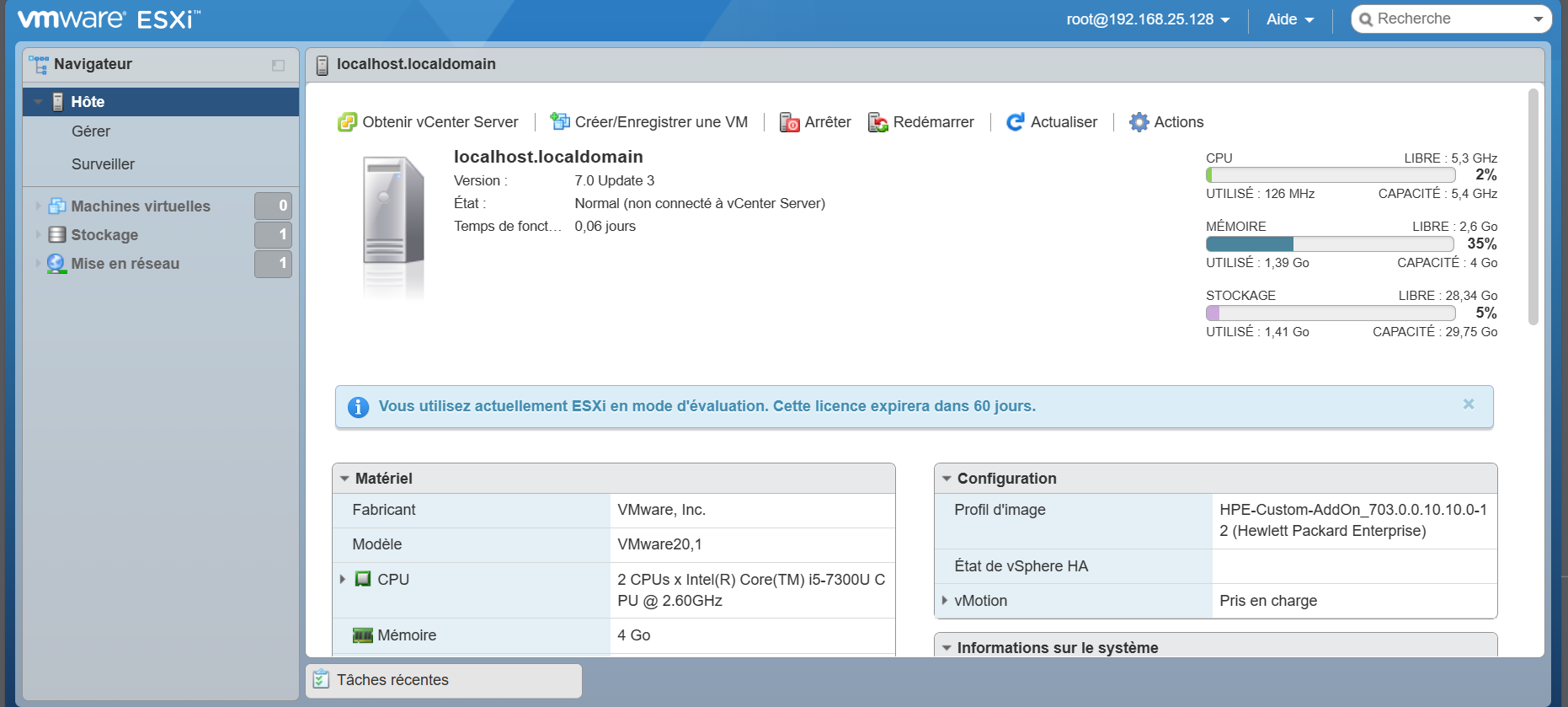
**Configuration**

**Firewall et sécurité**



**Lorsque vous installez l'hyperviseur VMware ESXi, une série de services sont présents sur celui-ci, dont une partie seulement est en cours d'exécution en temps normal.**  
**Pour autoriser et sécuriser l'accès à ces différents services, un pare-feu est préinstallé et préconfiguré sur votre hyperviseur VMware ESXi. Ce qui permet par défaut de bloquer les ports inutilisés actuellement par votre hyperviseur.**

Sur l’interface principale vous pouvoir voir tous les services disponibles sur hyperviseur que nous utilisons :



Dans la liste des services, vous trouverez notamment :

DCUI (Interface Utilisateur de la Console Directe) : qui correspond à la console jaune et grise que vous voyez à l'écran (si un écran est branché sur votre serveur).  
Notez que cette console DCUI peut aussi être utilisée via SSH en lançant le programme du même nom (dcui).

lwsmd (Service Active Directory) : service permettant de lier votre hyperviseur VMware ESXi à un domaine Active Directory.

ntpd (NTP) : service permettant de synchroniser la date et l'heure de votre hyperviseur depuis un serveur NTP (Network Time Protocol) de façon à ce que tous vos hyperviseurs (le cas échéant) puissent avoir exactement la même date et heure à la seconde près.  
Ce qui permet d'éviter certaines erreurs au niveau de l'authentification par exemple. Notamment si celui-ci est lié à un domaine Active Directory.

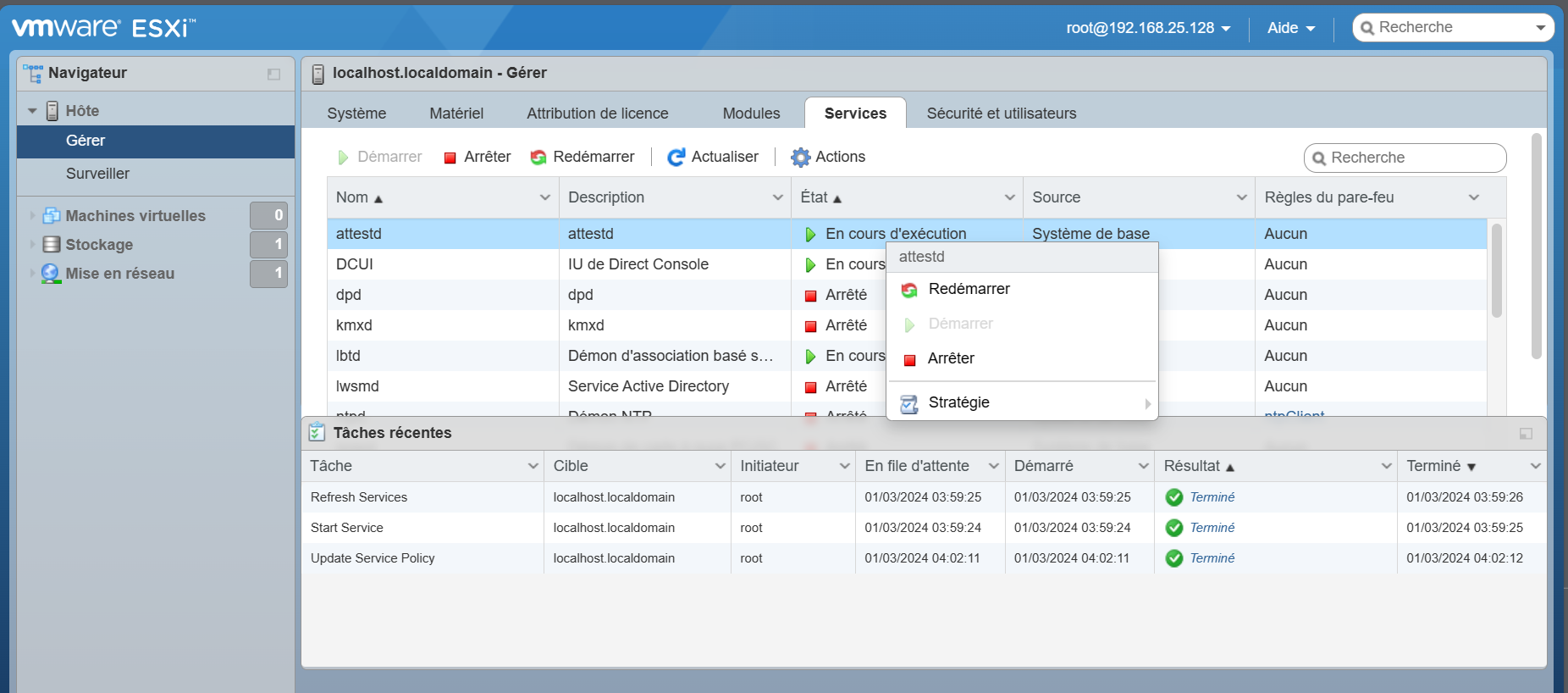
snmpd (Serveur SNMP) : service gérant l'envoi de notifications et permet de surveiller cet hyperviseur depuis des logiciels de monitoring

TSM (ESXi Shell) : service permettant de gérer votre hyperviseur VMware ESXi en ligne de commandes (depuis la console DCUI, par exemple).

TSM-SSH (SSH) : serveur SSH permettant de gérer votre hyperviseur VMware ESXi à distance en ligne de commandes (depuis un client SSH, tel que Putty) et/ou de gérer les fichiers et dossiers de celui-ci grâce au protocole SFTP (qui utilise le même port) avec un logiciel tel que WinSCP, par exemple.  
Pour en savoir plus, référez-vous à notre tutoriel : VMware ESXi 6.7 - Activer le protocole SSH.

vmsyslogd (Serveur Syslog) : service gérant l'enregistrement des messages provenant du VMKernel et d'autres composants système. Ces logs peuvent ensuite être transférés vers un autre collecteur de logs (tels que Syslog-NG, SexiLog, ...) si vous le souhaitez.

vxpa (Agent VMware vCenter) : permet de gérer la connexion de votre hyperviseur VMware ESXi à un serveur VMware vCenter.



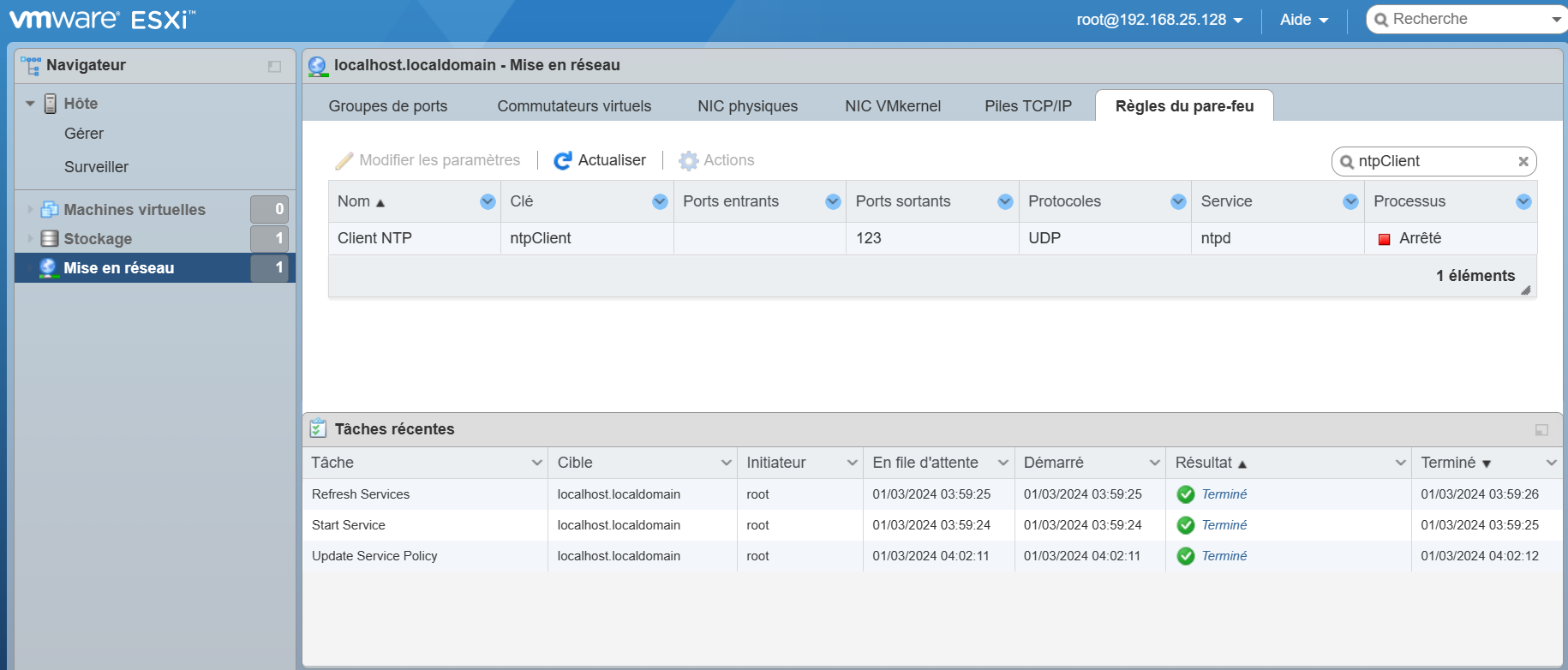
Pour chaque service, vous pourrez le démarrer, l'arrêter ou le redémarrer manuellement.

Ensuite, si vous cliquez sur "Actions", vous pourrez changer la stratégie de démarrage et d'arrêt à utiliser avec tel ou tel service :

Démarrer et arrêter avec les ports du pare-feu : si vous ouvrez les ports correspondant à ce service dans votre hyperviseur VMware ESXi, le service sera automatiquement démarré. Puis, arrêté lorsque vous fermerez les ports correspondant dans le pare-feu.

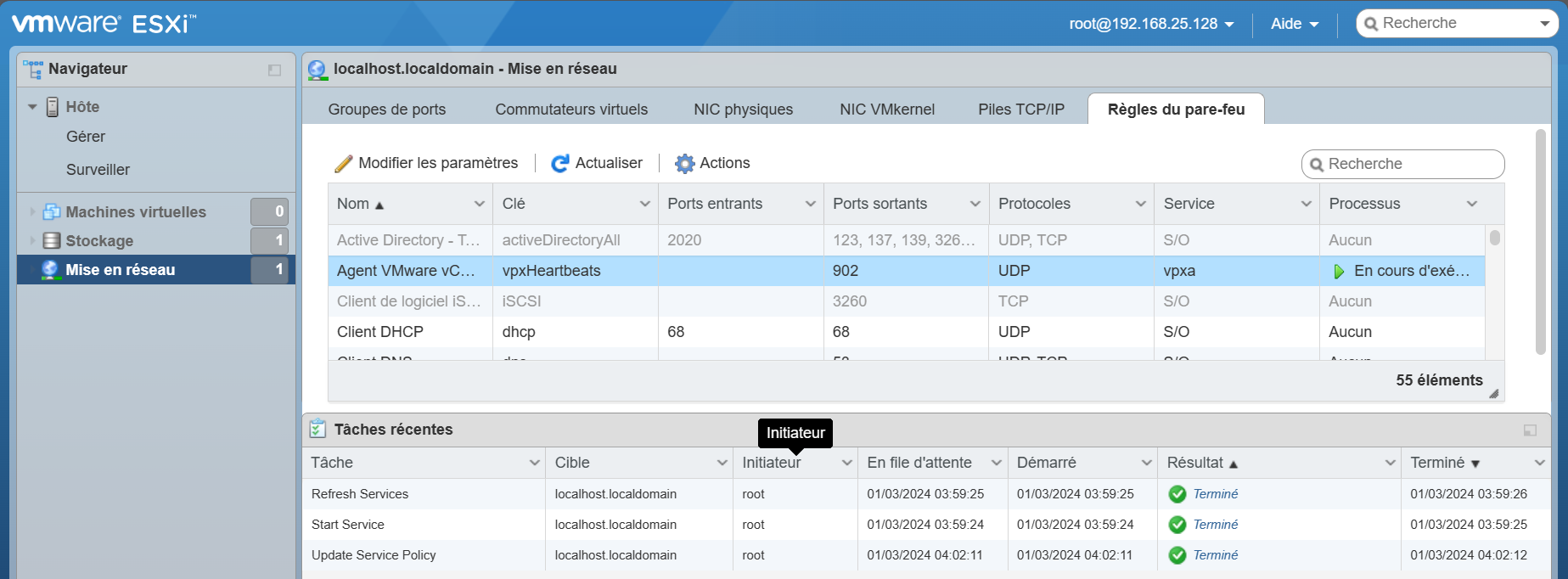
Démarrer et arrêter avec l'hôte : le service sera automatiquement démarré au démarrage de votre serveur et arrêté lors de l'arrêt du serveur

Démarrer et arrêter manuellement : aucun démarrage ou arrêt ne sera effectué automatiquement. Si vous souhaitez utiliser ce service, vous devrez le démarrer en cliquant sur "Démarrer".  
Ensuite, pour l'arrêter, cliquez sur "Arrêter". Notez tout de même que si vous arrêtez ou redémarrez votre serveur, ce service sera arrêté et il ne redémarrera pas automatiquement.



Pour certains services (dont "ntpd"), vous pourrez accéder à la règle correspondant dans le pare-feu en cliquant sur le lien présent dans la colonne "Règle du pare-feu".  
Pour ce service "ntpd", la règle est nommée "ntpClient".

En cliquant sur ce lien, vous serez redirigé automatiquement dans la section "Mise en réseau -> Règles du pare-feu" de cette interface web et le nom de la règle souhaitée sera automatiquement indiqué dans la case de recherche de façon à ce qu'elle apparaisse directement à l'écran.

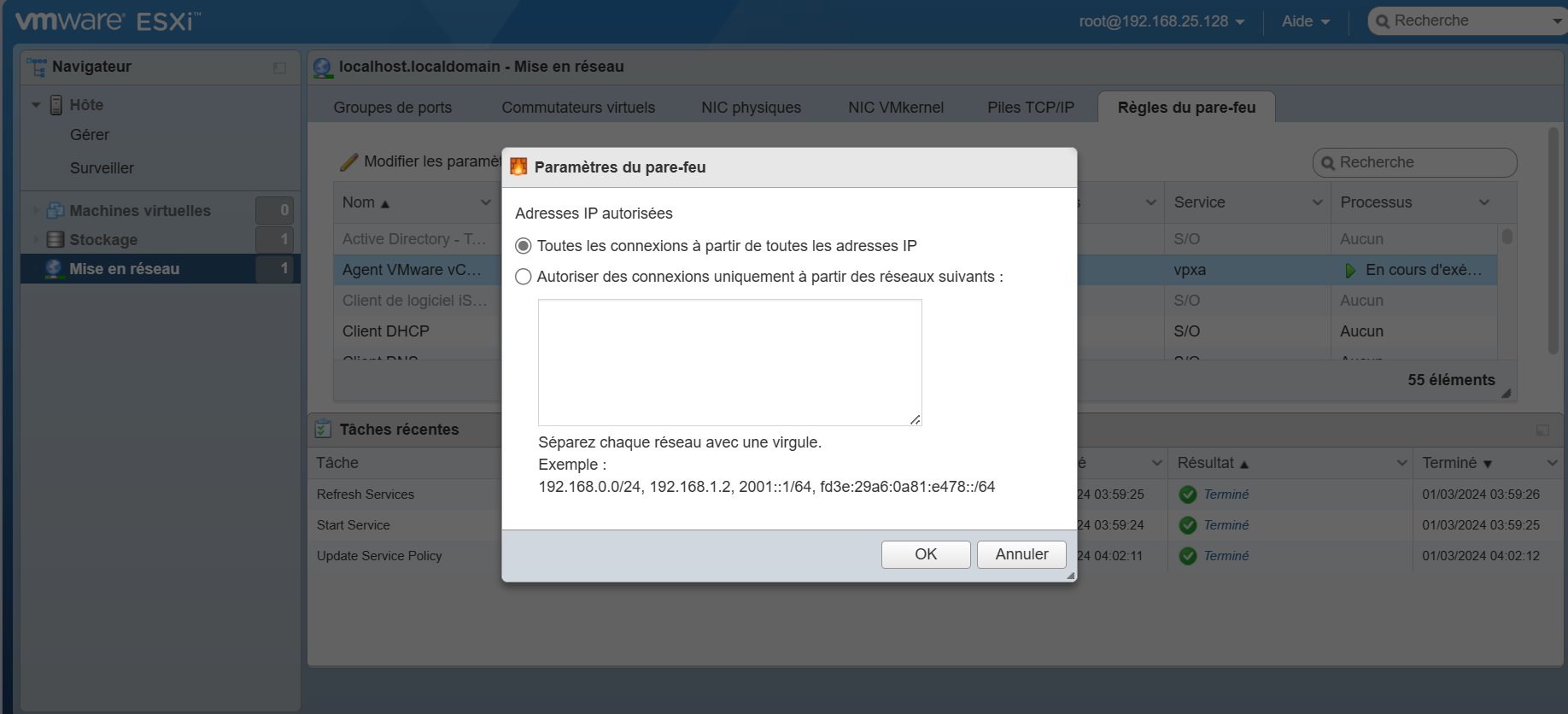


Pour modifier une règle de ce pare-feu, sélectionnez-la et cliquez sur "Modifier les paramètres".

Dans la fenêtre "Paramètres du pare-feu" qui apparait, vous pourrez choisir entre :

Toutes les connexions à partir de toutes les adresses IP : ce qui permet d'autoriser par défaut n'importe qui à se connecter sur le ou les ports concernés par cette règle.

Autoriser des connexions uniquement à partir des réseaux suivants : ce qui permet de limiter l'accès aux ports concernés par cette règle à certains réseaux et/ou à certains ordinateurs / serveurs spécifiques.  
Dans le cas de la règle "Serveur SSH", vous pourriez donc autoriser la gestion à distance de votre hyperviseur via SSH depuis uniquement certains ordinateurs pour éviter les attaques de pirates (par exemple).

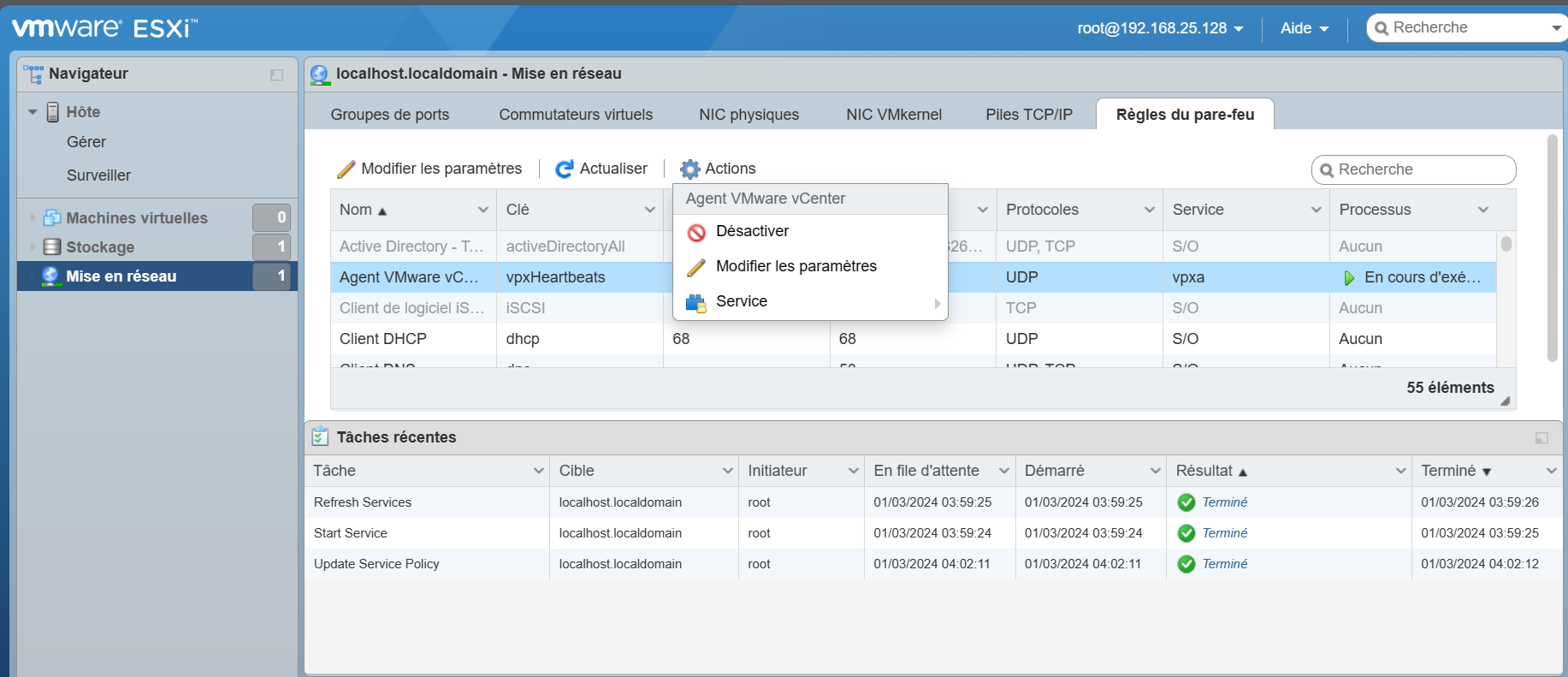


Pour limiter l'accès aux ports concernés par cette règle du pare-feu, sélectionnez "Autoriser des connexions uniquement à partir des réseaux suivants" et indiquez-le ou les réseaux et/ou l'adresse IP que vous souhaitez autoriser.

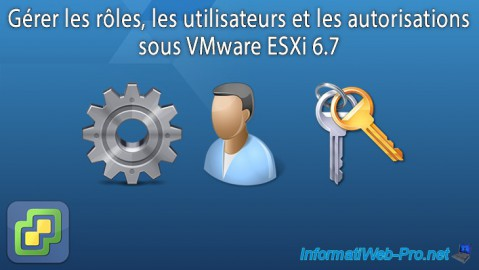
Pour chaque règle de ce pare-feu, vous pourrez cliquer sur "Actions" pour :

-Activer ou désactiver celle-ci

-Modifier les paramètres de celle-ci



**-utilisateurs et groups**



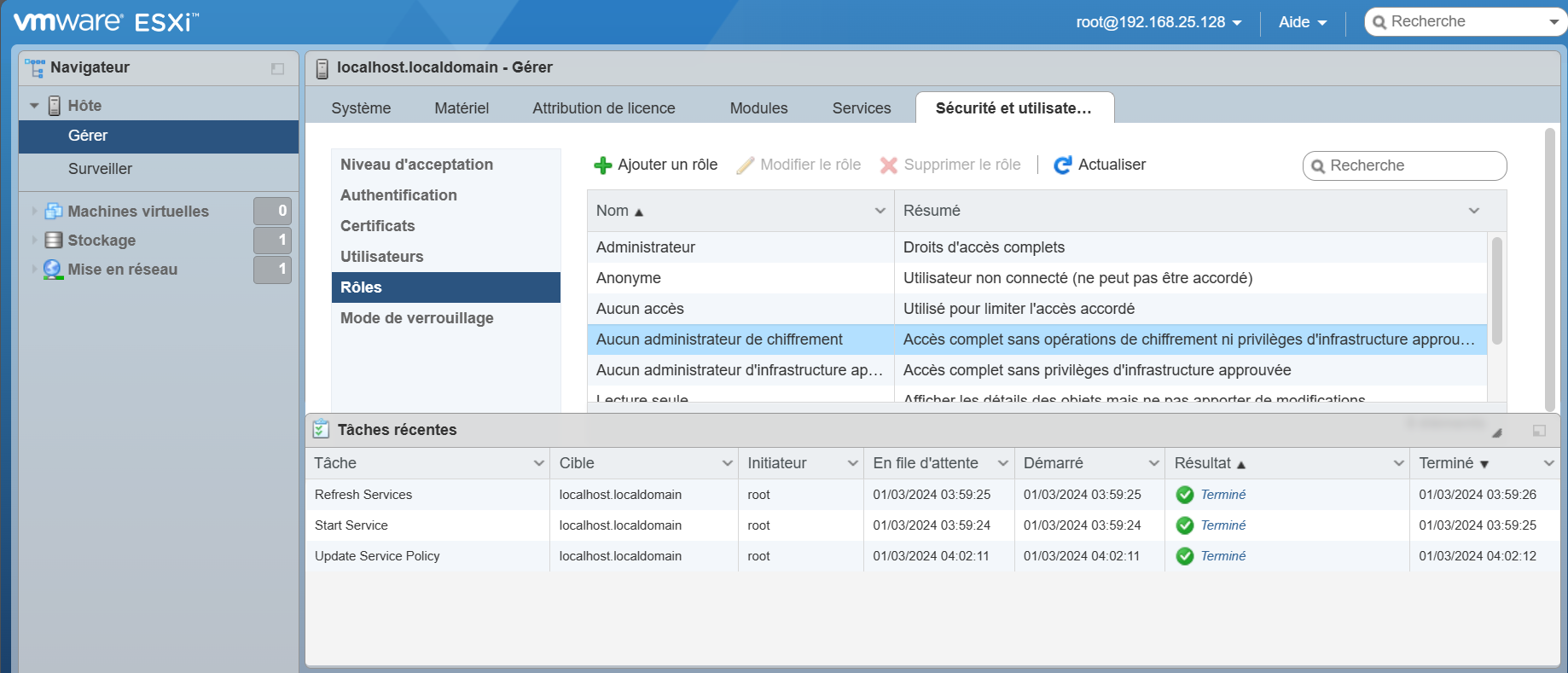
En tant qu'administrateur système (ou administrateur virtualisation, dans ce cas-ci), vous serez souvent appelé pour effectuer telle ou telle modification sur un serveur, un routeur, ...  
Dans le cas de VMware ESXi, comme avec d'autres technologies (dont l'Active Directory), il est possible de créer des utilisateurs supplémentaires avec des droits limités pour pouvoir déléguer certaines tâches courantes sans pour autant permettre à l'utilisateur de faire n'importe quoi.

Pour déléguer certaines tâches à des personnes de confiance (qu'il s'agisse de responsables ou d'employés), vous devrez toujours utiliser une combinaison de 3 éléments : comptes d'utilisateurs, rôles et autorisations.

Pour pouvoir accorder tel ou tel droit à un utilisateur sur tel ou tel objet, VMware ESXi utilise un système de rôles.  
Pour voir la liste des rôles disponibles par défaut, allez dans : Hôte -> Gérer -> Sécurité et utilisateurs -> Rôles.

Comme vous pouvez le voir, par défaut, VMware ESXi propose différents rôles :

* Administrateur : permet de donner tous les droits à un utilisateur sur un objet (qu'il s'agisse de l'hyperviseur dans son entièreté, ou une machine virtuelle spécifique, ou tout autre objet).
* Anonyme : correspond aux droits que possède un "utilisateur" non connecté. Notez que ce droit ne peut pas être accordé et qu'il ne sera donc pas visible dans le menu "Actions -> Autorisations" des objets souhaités.
* Aucun accès : permet de limiter (supprimer) les droits qu'un utilisateur avait sur un objet enfant grâce à des droits que vous lui auriez accordés sur un objet parent.
* Aucun administrateur de chiffrement : possède quasiment les mêmes droits que le rôle "Administrateur" à l'exception des opérations de chiffrement qui ne seront pas possibles avec ce rôle.
* Lecture seule : permet de voir diverses informations (en fonction de l'objet concerné), mais l'utilisateur ne pourra apporter aucune modification sur les objets concernés.
* Afficher : similaire au rôle précédent (Lecture seule), mais à la différence que celui-ci ne peut pas être accordé. Il ne sera donc pas visible depuis la fenêtre de gestion des autorisations sur l'objet souhaité.



Bien qu'il existe des rôles par défaut avec des permissions prédéfinies pour ceux-ci, vous pouvez aussi créer vos propres rôles pour pouvoir gérer l'attribution de permissions plus en détail.  
Pour cela, cliquez sur : Ajouter rôle.

Pour ajouter un rôle, vous devrez :

Nom du rôle (requis) : indiquer un nom pour celui-ci

Privilèges : choisir les privilèges que vous souhaitez accorder à vos futurs utilisateurs grâce à ce rôle

Comme vous pouvez le voir, vous pourrez accorder ou non des privilèges pour :

Datastore : la gestion des banques de données. Pour autoriser ou non des utilisateurs à gérer les fichiers, les déplacer, les supprimer, allouer de l'espace (nécessaire pour créer un disque dur virtuel, par exemple), ...

Network : la gestion des réseaux. Configurer des réseaux, en supprimer, en assigner, ...

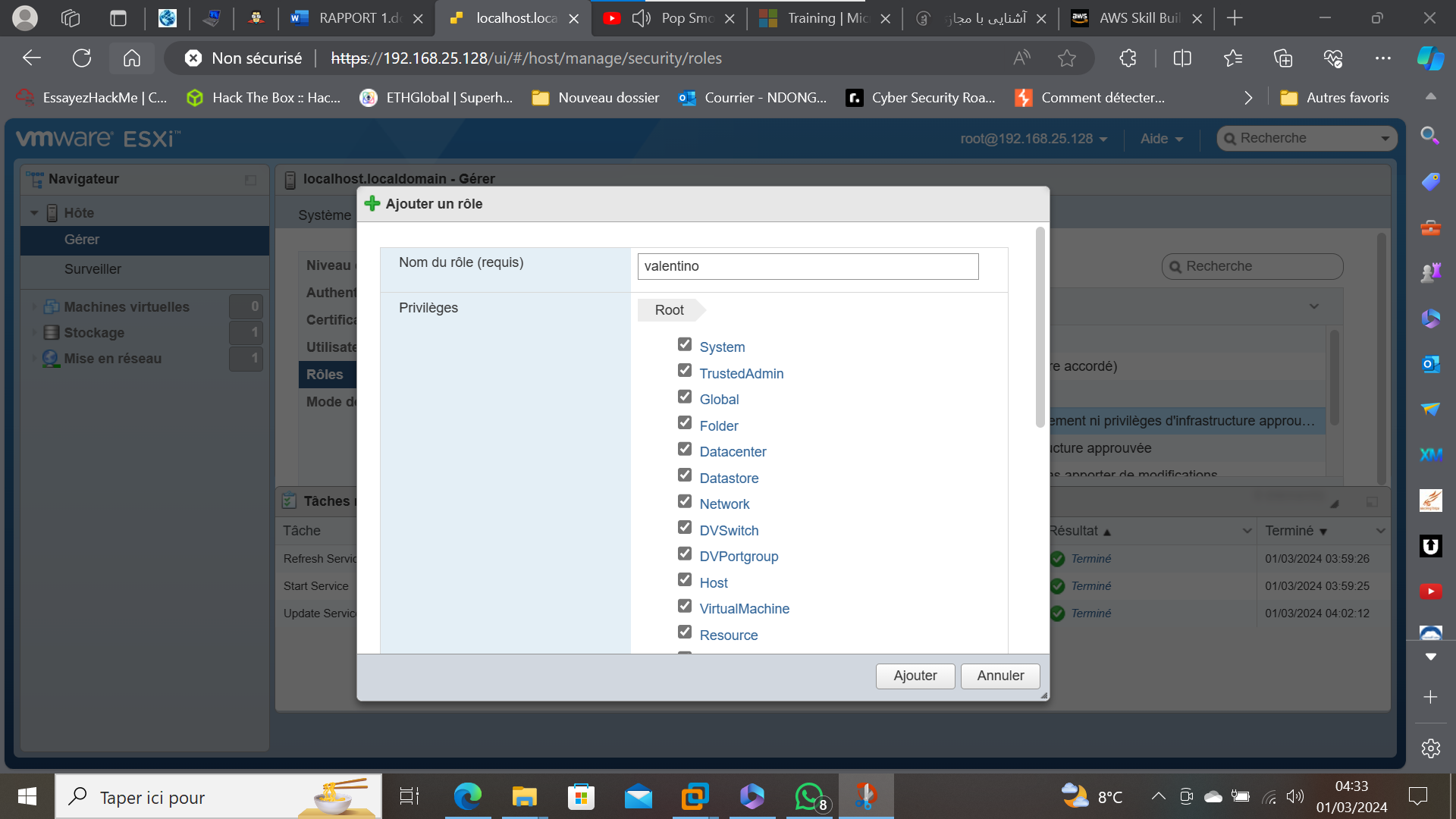
Host : la gestion de l'hôte (l'hyperviseur VMware ESXi)

VirtualMachine : la gestion de machines virtuelles.

Authorization : la gestion des rôles et des autorisations.

Certificate : la gestion de certificats numériques.

etc.



Une fois que vous aurez regroupé les différents privilèges à accorder à vos futurs utilisateurs grâce aux rôles, vous devrez créer des comptes d'utilisateurs pour ceux-ci.  
En entreprise, la création d'utilisateurs permet d'accorder différents droits en fonction des utilisateurs, mais aussi de contrôler ce que font ceux-ci.  
Ainsi, en cas de problème, vous pourrez facilement savoir quelle personne a fait une mauvaise manipulation ou quelque chose qu'elle n'aurait pas du faire.

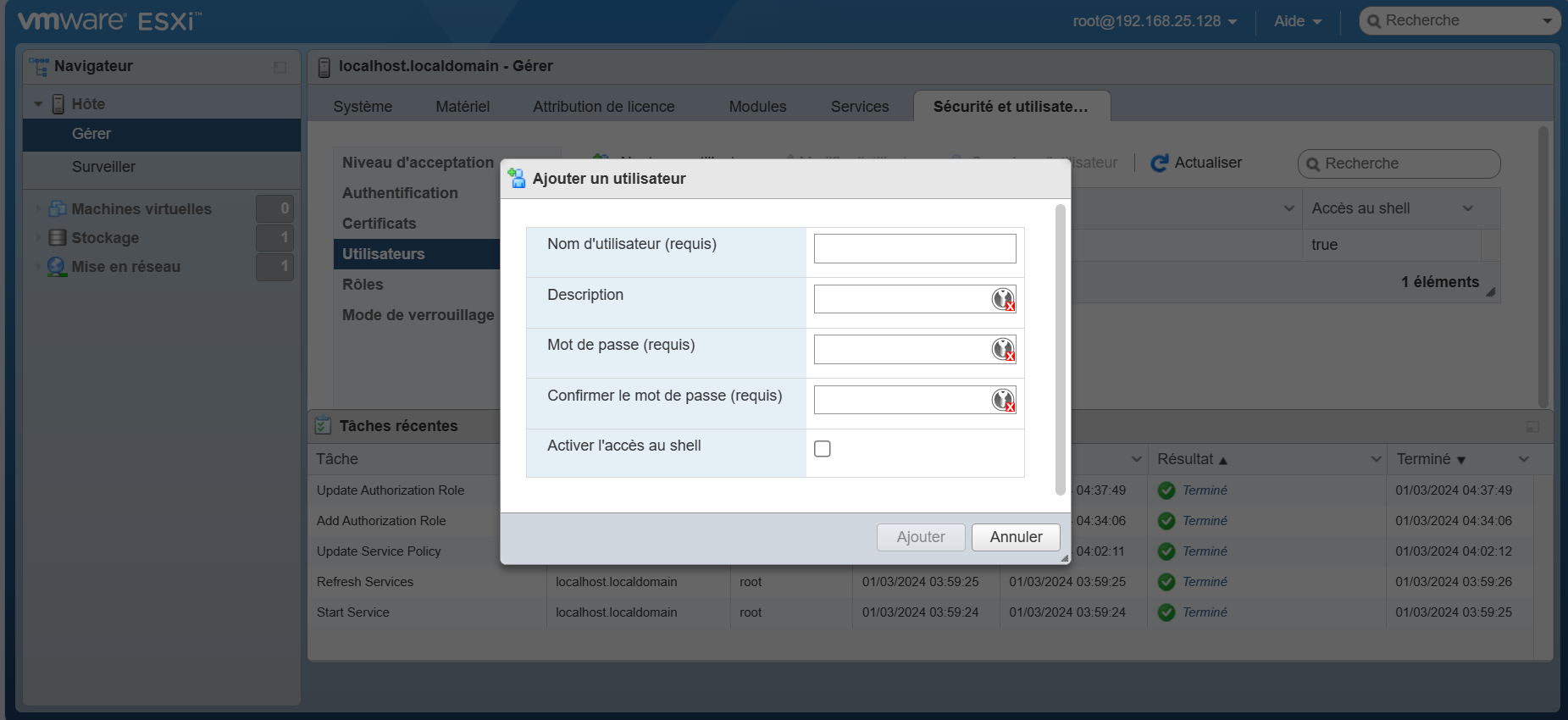
Pour gérer les utilisateurs de votre hyperviseur VMware ESXi, allez dans : Hôte -> Gérer -> Sécurité et utilisateurs -> Utilisateurs.  
Comme vous pouvez le voir, par défaut, seulement le compte "root" est présent dans cette liste d'utilisateurs.

Dans la fenêtre "Ajouter un utilisateur" qui apparait, indiquez :

Nom d'utilisateur (requis) : le nom d'utilisateur qu'il ou elle devra utiliser pour se connecter au serveur VMware ESXi

Description : une description pour savoir de qui il s'agit (facultatif)

Mot de passe : 2 fois un mot de passe pour celui-ci.  
Notez que par défaut, VMware ESXi requiert que le mot de passe possède au moins 7 caractères (dont au moins 1 minuscule, 1 majuscule, 1 chiffre et un caractère spécial).  
Néanmoins, si vous souhaitez diminuer cette complexité pour permettre à vos utilisateurs d'utiliser des mots de passe moins compliqués, vous pouvez le faire en suivant notre tutoriel : VMware ESXi 6.7 - Changer la complexité requise pour les mots de passe.

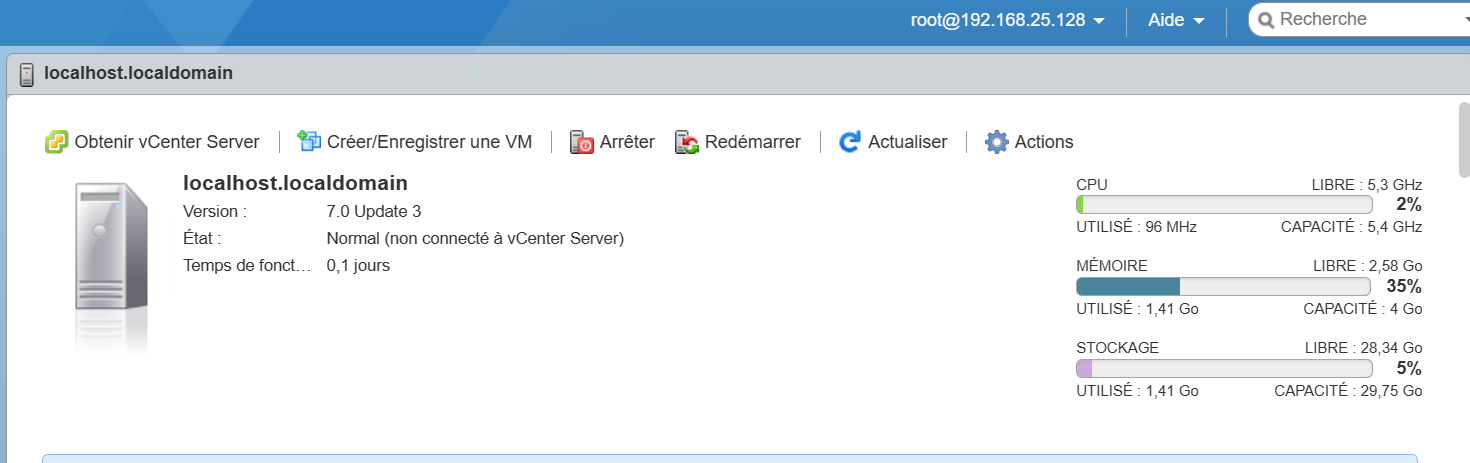


**-Ajouts (réseaux,disque,ports)**



Pour commencer, sur la page d'accueil (accessible via le menu "Hôte" à gauche), vous pouvez surveiller l'utilisation du processeur (CPU) via les informations affichées en haut à droite.  
Vous pouvez voir la fréquence utilisée (en MHz/GHz ou en %), sa capacité totale (en MHz/GHz) et ce qui est disponible (en MHz/GHz).  
Notez que l'utilisation apparait en vert (uniquement si le processeur est un minimum utilisé).

Notez que la capacité en GHz affichée par VMware ESXi correspond à la fréquence de base de votre processeur (dans notre cas : 3 GHz) multipliée par le nombre de coeurs physiques de votre processeur.

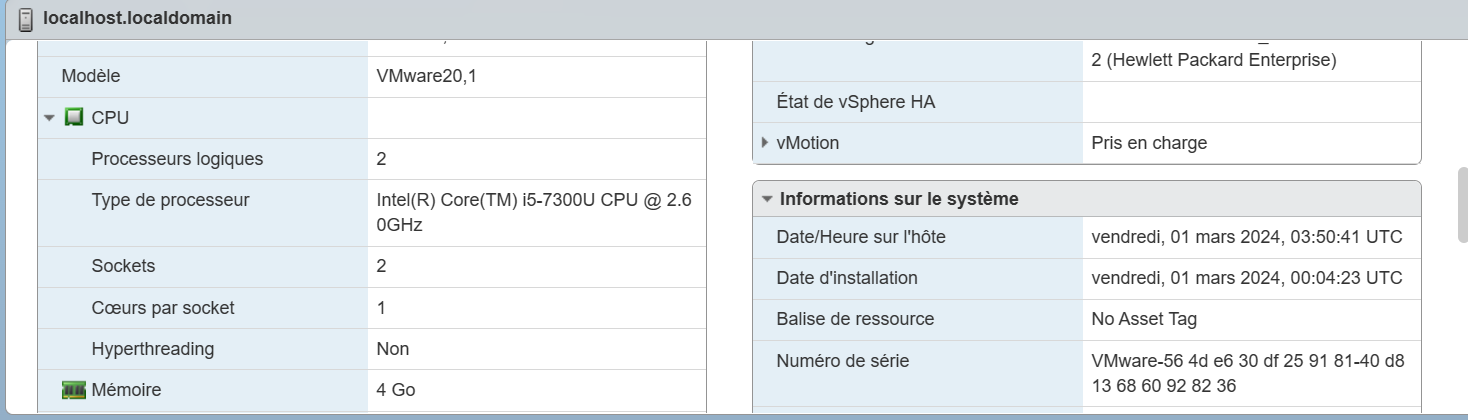


Si vous allez dans le menu "Hôte -> Surveiller", vous verrez par défaut le graphique concernant le processeur (CPU).  
Comme vous pouvez le voir, ce graphique vous permet de surveiller :

[Nom de votre hôte ESXi] : l'utilisation globale de tous les processeurs de votre serveur (dans le cas où vous en auriez plusieurs).

Module X : l'utilisation de chaque processeur physique (socket) de votre serveur

Notez que VMware ESXi ne peut afficher que l'historique d'utilisation pour la dernière heure d'utilisation.  
Pour avoir un historique plus long, vous aurez besoin de VMware vCenter Server (VCSA).



Si vous le souhaitez, vous pouvez cliquer sur l'option "Sélectionner des VM" pour ajouter des machines virtuelles sous tension (allumées) dans ce graphique.

