Surveillance

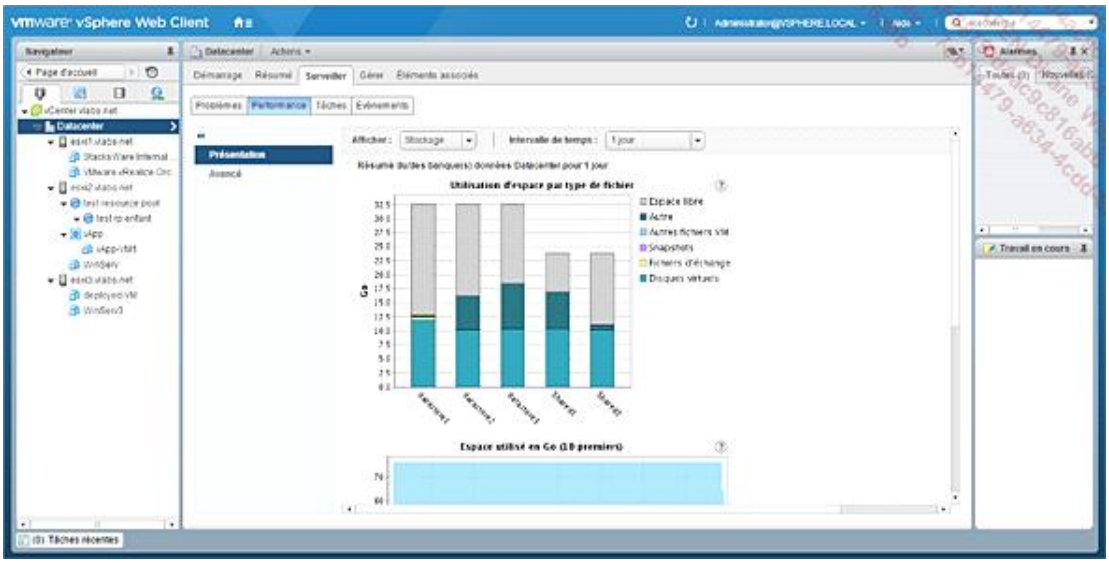
Il y a pléthore d'outils pour surveiller l'état de l'environnement vSphere, dont certains sont intégrés au sein du serveur vCenter. D'autres sont fournis par l'éditeur. Certains produits spécialisés sont même capables de faire des planifications en se basant sur l'utilisation des ressources (capacity planning).

Le but de cette section est de présenter certains de ces outils, et leurs spécificités le cas échéant.

1. Graphes vCenter

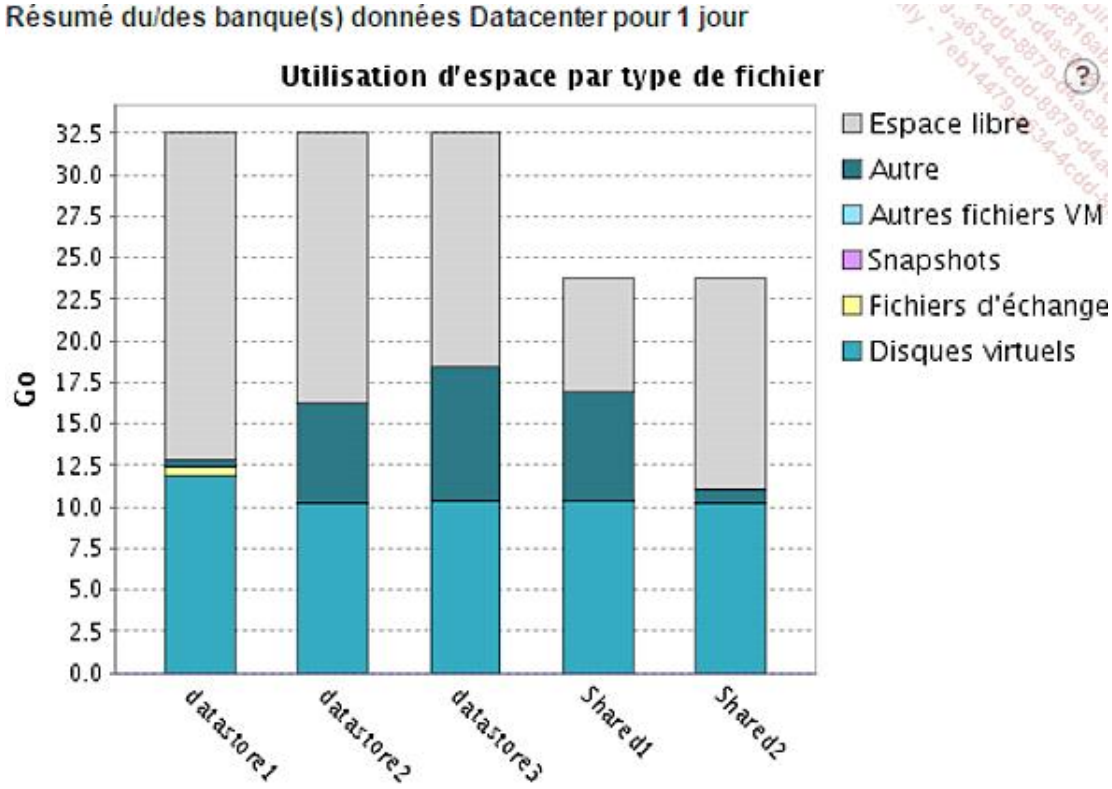
vCenter est le premier outil à utiliser pour observer son environnement. Des graphes sont inclus et permettent de surveiller l'utilisation des ressources au sein de l'inventaire. Ils peuvent être consultés sur l'onglet **Surveiller** du Web Client.

Les vues dépendent de l'objet choisi dans la partie navigateur de l'interface, ici le datacenter :

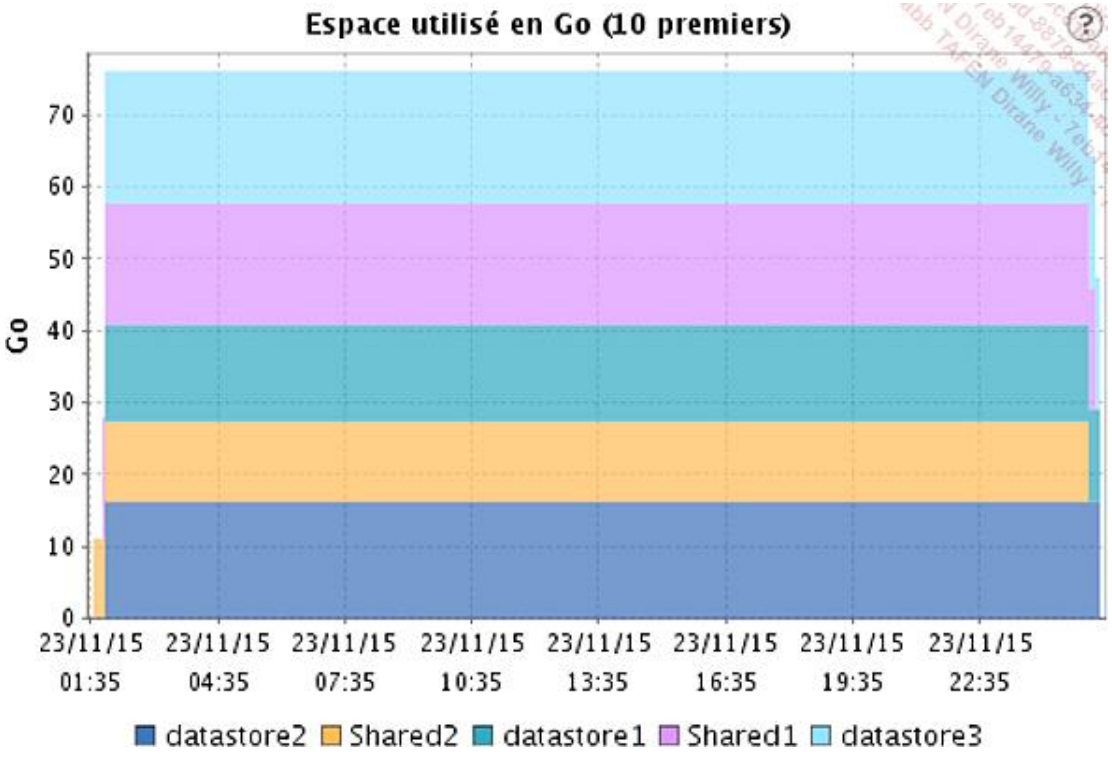


La vue par défaut est la « présentation » associée au stockage. On voit par exemple des informations concernant la consommation d'espace disque.

En détail :

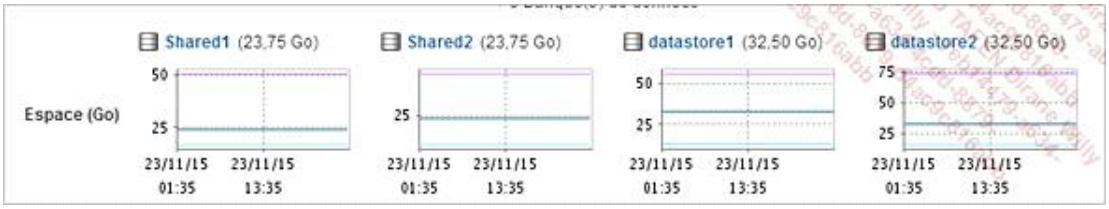


On peut observer la répartition des différents types de fichiers présents dans chaque datastore.

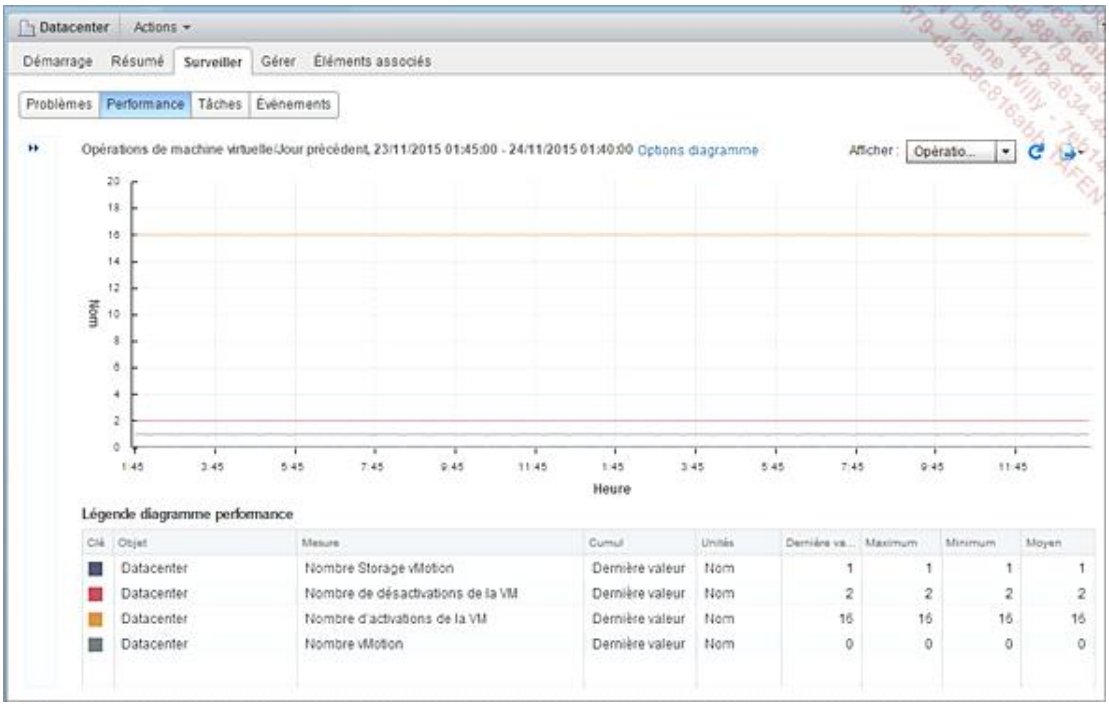


Ici, il s'agit d'un classement des datastores selon l'espace consommé.

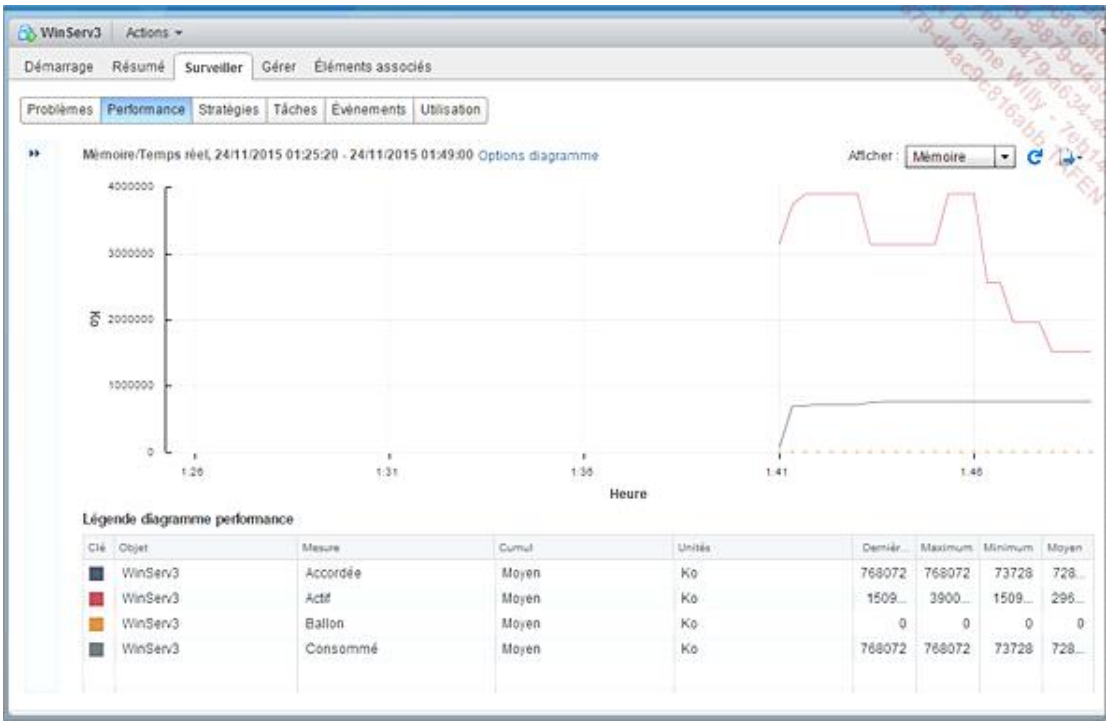
La partie avancée permet d'afficher de petits graphiques centrés sur chacun des datastores (nous sommes toujours sur la vue stockage) :



Les opérations effectuées sur différents objets de l'inventaire sont disponibles :



Tout comme les informations de performance :



Concernant ici la machine virtuelle WinServ3.

Toutes les informations affichées sous forme de courbes, de piles ou de camemberts sont des informations collectées et enregistrées dans la base de données du vCenter. La base est prévue pour conserver les données sur une année. De même, la période maximale d'affichage des données dans le client vSphere (web ou Windows) est d'une année.

Gardez à l'esprit que plus le temps passe, plus on perd en précision sur l'information enregistrée : si on revient en arrière sur quelques minutes on obtient une collecte toutes les 20 secondes. Si on revient consulter une donnée vieille de quelques mois, il n'y aura plus qu'un point par jour car pour éviter de remplir la base de données, les statistiques sont traitées par périodes pour lesquelles des moyennes sont calculées. Ce qui aujourd'hui est un pic rapide de consommation de ressources pourra être vu dans quelques mois comme une augmentation modérée.

Voici les informations de collectes de données pour vCenter par défaut :

Intervalle	Fréquence
1 jour	5 minutes
1 semaine	30 minutes
1 mois	2 heures
1 an	1 jour

Il est possible de créer ses propres graphiques avec un choix d'indicateurs et de les conserver pour une utilisation ultérieure.

Concernant ces indicateurs, les plus couramment observés sont :

- Utilisation de processeur,
- Utilisation de mémoire vive,
- Ballooning (mémoire transférée grâce au pilote vmmemctl alias balloon driver).

Le détail des différents indicateurs et la manière de les traiter sont traités dans le document officiel vSphere Monitoring and Performance - vSphere 6.0 - VMware disponible à l'adresse suivante : https://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-601-monitoring-performance-guide.pdf

2. ESXTOP

ESXTOP est un utilitaire de surveillance système disponible pour les hyperviseurs. Il dérive de TOP sous Linux. L'intérêt d'utiliser top est que les informations évoluent en temps réel (enfin presque).

ESXTOP est accessible via la ligne de commande directement sur l'hyperviseur (en ayant activé la console locale - le mode support), la console distante (l'accès SSH) ou en passant par la vMA ou vSphere Management Apppliance (ou Assistant).

Dans le cas de vMA on parle de rESXTOP pour remote ESXTOP (ESXTOP à distance).

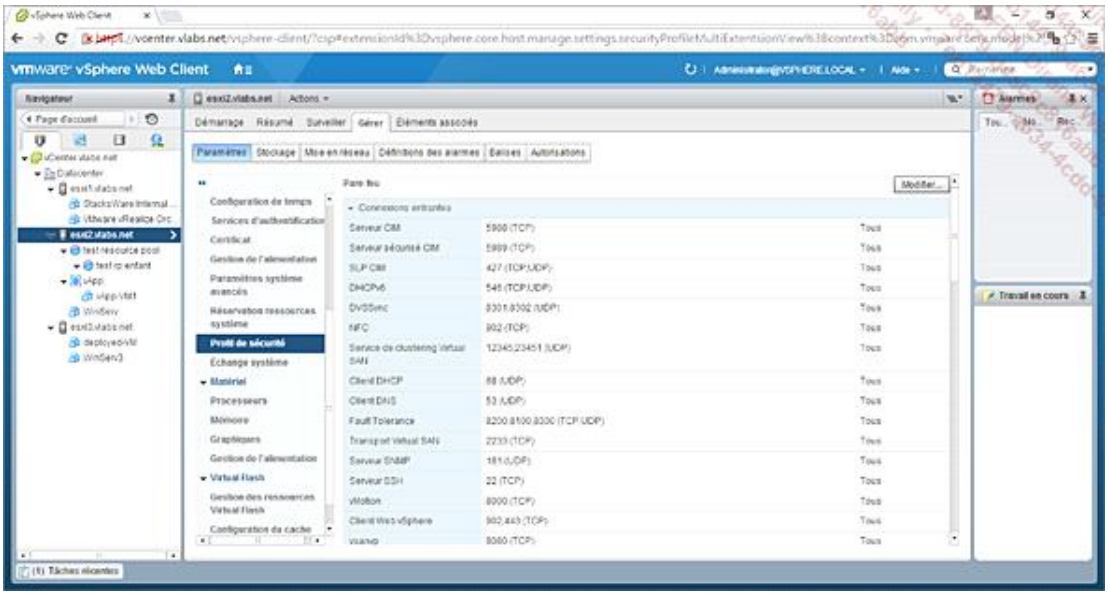
a. Activation de SSH sur un serveur hôte

L'accès SSH n'est pas activé par défaut sur les serveurs ESXi. Il s'agit d'une mesure de sécurité au nom du principe

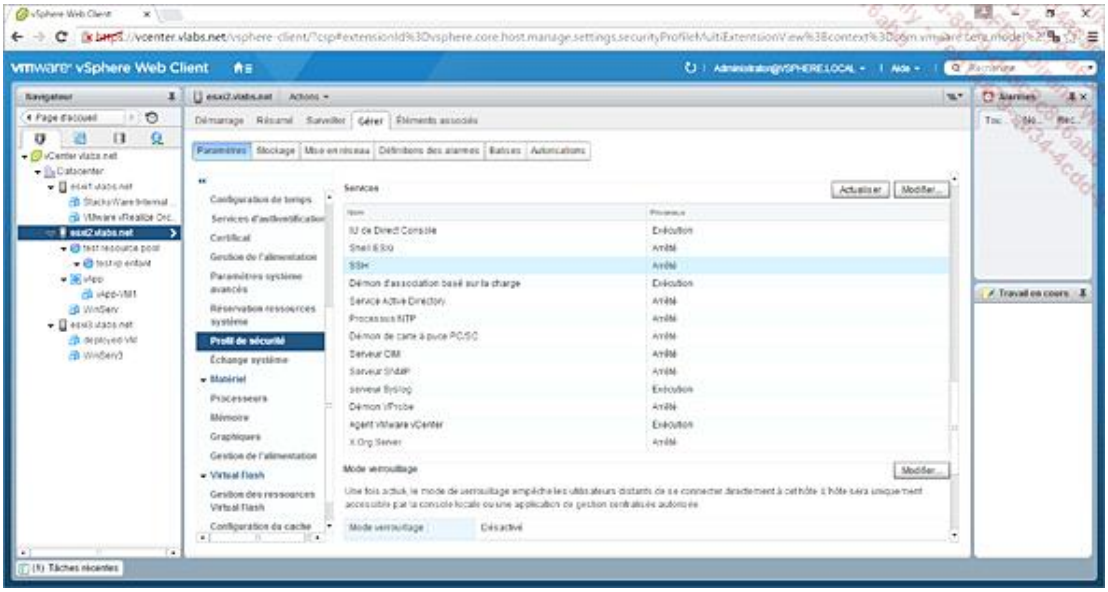
de réduction de la surface d'exposition : si vous n'avez pas besoin d'un service sur un système, désactivez-le car il pourrait être une porte d'entrée pour des personnes mal intentionnées via des failles connues ou exploits.

Dans le domaine de la sécurité informatique, un exploit est un bout de code (programme) permettant d'exploiter une faille dans un système ou logiciel informatique.

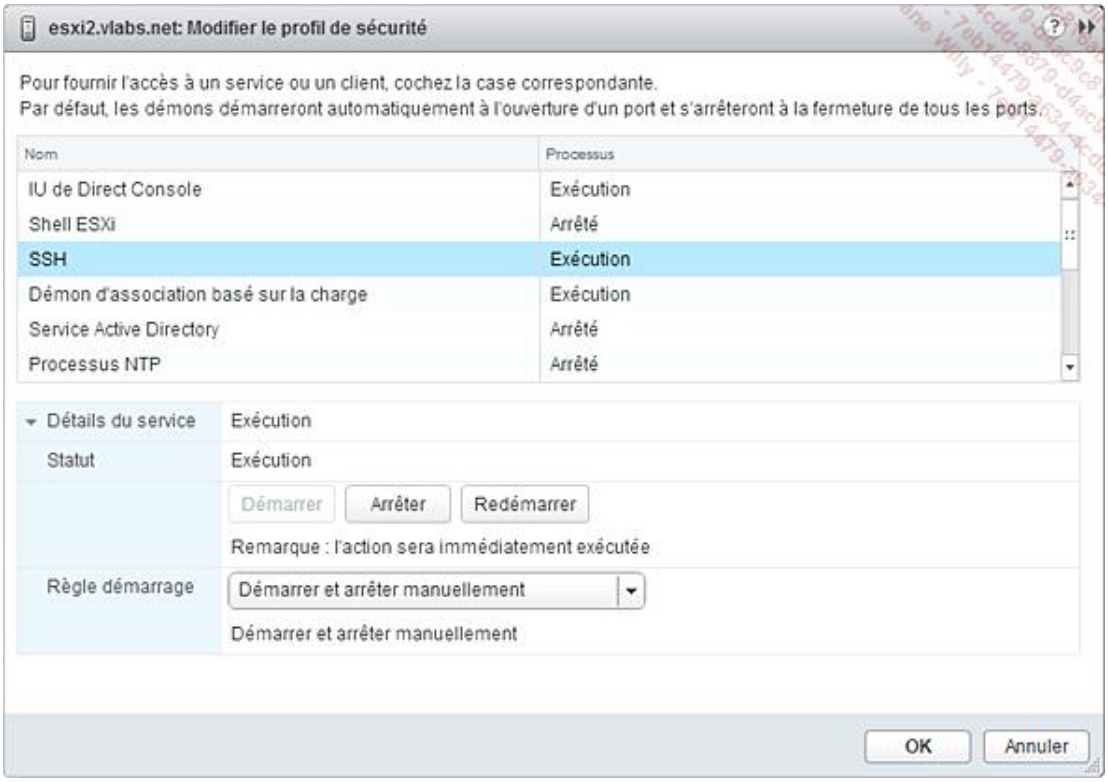
De base le profil de sécurité permet de connaître les services activés et désactivés sur un hyperviseur. Le cas échéant, il est possible d'activer et démarrer des services supplémentaires et d'ouvrir/fermer des ports :



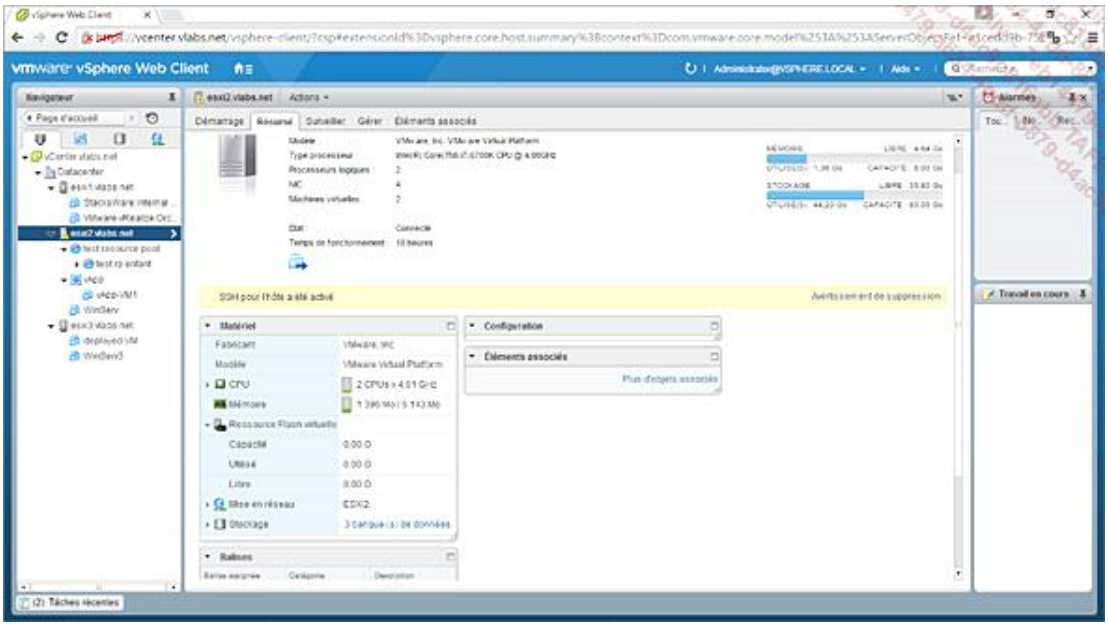
En sélectionnant le service SSH :



On voit que le service est arrêté.



En modifiant le profil, on peut démarrer le service SSH. Attention à la règle de démarrage si on souhaite que le service soit démarré en même temps que l'hyperviseur !



On remarque la présence d'un avertissement, car en plus de la considération sécuritaire, un service supplémentaire consomme de la ressource.

b. vMA

L'appliance vMA comprend la ligne de commande vSphere (vCLI) ainsi que le SDK pour Perl et permet de passer des commandes et scripts sur les serveurs ESXi en passant par vCenter ou non. vMA gère l'authentification via un élément interne (Fastpass) ou via Active directory.

vMA est disponible sous forme OVF à l'adresse suivante : https://www.vmware.com/support/developer/vima/ (un compte myVMware est requis).

Avec la vMA, l'activation de SSH sur les serveurs hôtes n'est pas nécessaire car vMA utilise les API VMware pour les communications avec vCenter et les serveurs ESXi. Voici pour information l'initialisation après un déploiement de l'appliance vMA.

Nous ciblons notre vCenter ou notre ESXi via la commande suivante :

```
vifp addserver %cible% --authpolicy %authentification%
--username %utilisateur%
```

`%authentification%` correspond au mode d'authentification via Active Directory (adauth) ou FastPass (fpauth).

Pour plus d'information sur les modes d'authentification, VMware fournit un tableau descriptif : https://pubs.vmware.com/vsphere-65/index.jsp#com.vmware.vma.doc/GUID-10F418CE-76DC-4AB9-AC50-52BEAF60BED0.html

Nous pouvons ensuite exécuter à distance des commandes comme si nous étions dans un shell SSH.

c. Introduction à l'utilisation d'ESXTOP

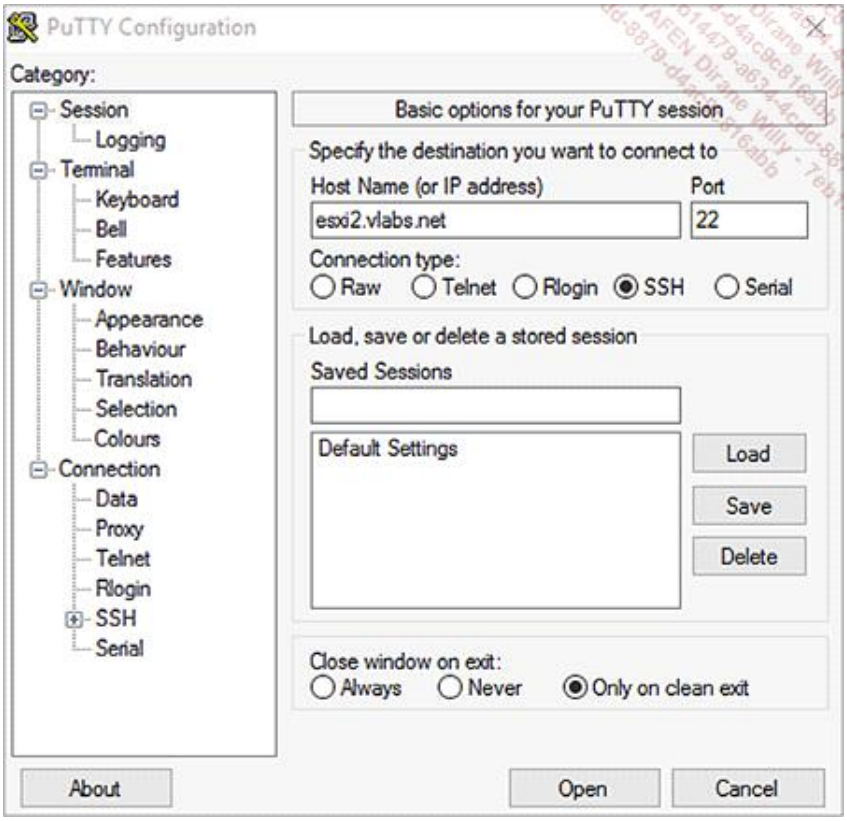
ESXTOP est un outil permettant d'observer l'utilisation des ressources sur un hyperviseur ESX. Il est similaire à l'utilitaire top que l'on trouve au sein des systèmes Unix, Linux et macOS.

```
Processes: 284 total, 2 running, 282 sleeping, 1038 threads                    15:39:15
Load Avg: 1.65, 1.49, 1.40  CPU usage: 0.85% user, 1.46% sys, 97.68% idle
SharedLibs: 265M resident, 52M data, 28M linkedit.
MemRegions: 39286 total, 3467M resident, 187M private, 909M shared.
PhysMem: 7963M used (1753M wired), 8416M unused.
VM: 777G vsize, 621M framework vsize, 0(0) swapins, 0(0) swapouts.
Networks: packets: 60731/58M in, 51078/7100K out. Disks: 74682/3849M read, 47292/4343M written.

PID   COMMAND      %CPU  TIME     #TH   #WQ  #PORT MEM    PURG   CMPR PGRP PPID STATE
1034  screencaptur 0.6   00:00.30 2     1    53    2808K  20K    0B   280  280  sleeping
1032  com.apple.Di 0.0   00:00.02 2     2    33    1268K  0B     0B   1032 1    sleeping
1030  top          1.8   00:00.82 1/1   0    22    3332K  0B     0B   1030 1023 running
1029  mdworker     0.0   00:00.04 3     1    53    3212K  0B     0B   1029 1    sleeping
1023  bash         0.0   00:00.00 1     0    16    768K   0B     0B   1023 1022 sleeping
1022  login        0.0   00:00.01 2     1    29    1096K  0B     0B   1022 1020 sleeping
1021  MTLCompilerS 0.0   00:00.06 2     2    32    13M    0B     0B   1021 1    sleeping
1020  Terminal     0.5   00:01.70 13    8    255   32M    132K   0B   1020 1    sleeping
1019  com.apple.Sa 0.0   00:00.06 3     2    42    5084K  0B     0B   1019 1    sleeping
997   mdworker     0.0   00:00.09 3     1    56    4552K  56K    0B   997  1    sleeping
996   mdworker     0.0   00:00.09 3     1    56    4548K  60K    0B   996  1    sleeping
995   mdworker     0.0   00:00.09 3     1    56    4660K  56K    0B   995  1    sleeping
993   mdworker     0.0   00:00.10 3     1    56    4700K  76K    0B   993  1    sleeping
992   mdworker     0.0   00:00.19 3     1    59    7084K  268K   0B   992  1    sleeping
991   mdworker     0.0   00:00.11 3     1    59    5212K  140K   0B   991  1    sleeping
990   mdworker     0.0   00:00.12 3     1    59    5056K  172K   0B   990  1    sleeping
987   MTLCompilerS 0.0   00:00.04 2     2    32    9632K  0B     0B   987  1    sleeping
986   Notes        0.0   00:03.73 13    1    285   84M    15M    0B   986  1    sleeping
958   AirPort Base 0.0   00:00.01 3     1    42    1104K  0B     0B   958  1    sleeping
957   netbiosd     0.0   00:00.02 2     2    30    2580K  0B     0B   957  1    sleeping
881   MTLCompilerS 0.0   00:00.02 2     2    31    5340K  0B     0B   881  1    sleeping
```

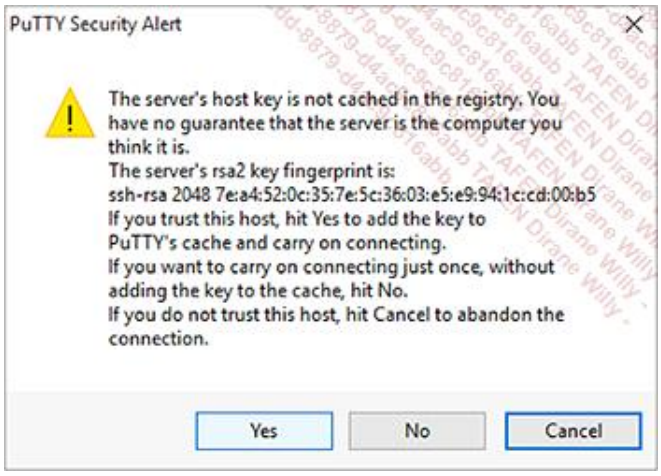
Capture d'écran de top sur macOS (10.12 Sierra)

Pour utiliser top : on se connecte à l'ESXi via SSH (ou on se connecte directement à la console de l'hyperviseur concerné :

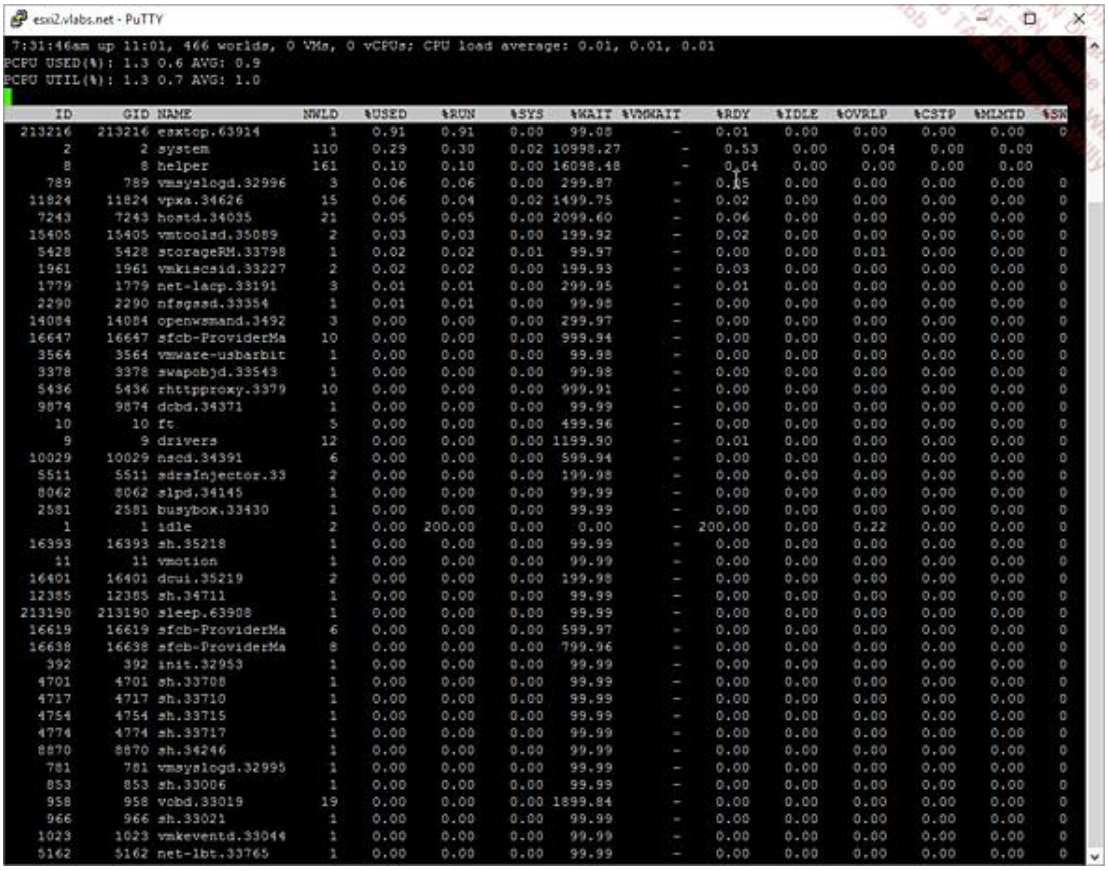


Ici, la connexion est faite à partir d'un poste Windows et SSH (*remote technical support*) est activé sur le serveur hôte.

L'alerte de sécurité est affichée à la première connexion. Il convient de vérifier l'empreinte du serveur directement sur celui-ci pour s'assurer qu'on se connecte sur la bonne machine :

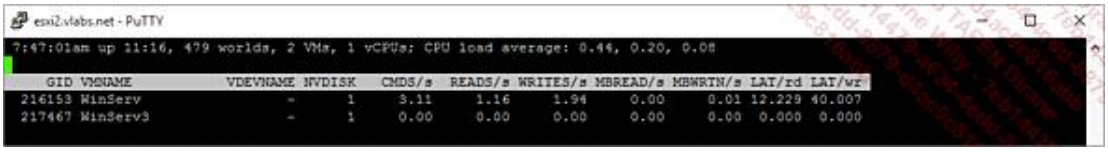


À la connexion, on arrive sur un écran présentant une liste des différents processus en cours sur la machine :

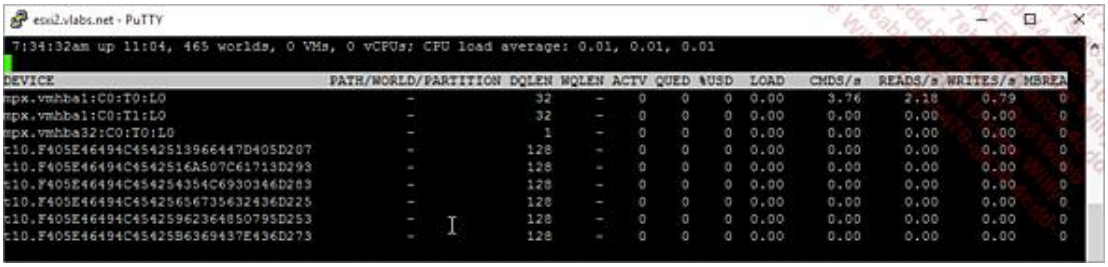


La vue est axée sur la consommation CPU, il y a cependant beaucoup de colonnes. Pour les filtrer, utiliser la touche [f] (comme fields ou champs à afficher) :

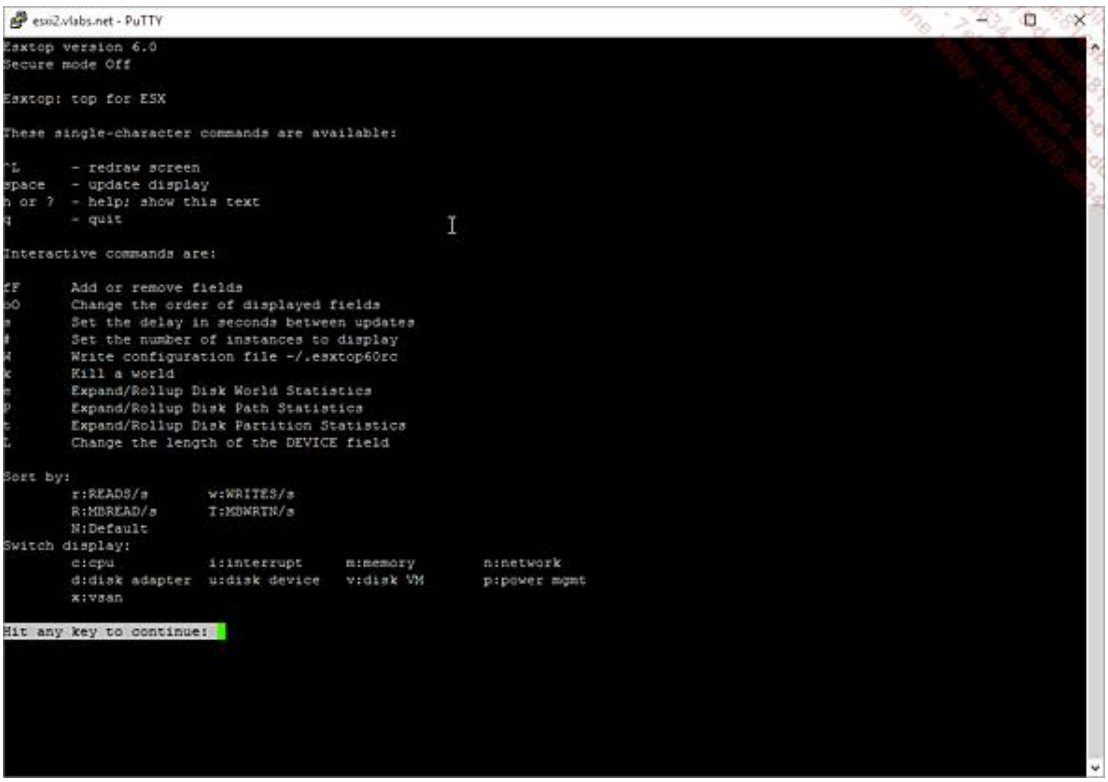
Pour afficher le détail concernant les machines virtuelles : utiliser la touche [V] :



En ce qui concerne le stockage : utiliser la touche [u] (disk device) :



N'hésitez pas à consulter l'aide pour tous les raccourcis (attention, certains sont en majuscules, d'autres en minuscules et d'autres fonctionnent indifféremment comme o ou O) :



Il est aussi possible de changer l'échantillonnage par défaut qui est de 5 secondes (une mise à jour des valeurs toutes les 5 secondes) et d'utiliser ESXTOP pour enregistrer des évolutions de valeurs sur un temps donné, puis les rejouer plus tard.

On utilise la commande `esxtop -b -d 3 -n 50 > ESXIESXTOP.csv` à cette fin : le paramètre `-b` est pour batch, `-d 3` pour une prise de mesure toutes les 3 secondes, `-n 50` indique que l'on veut capturer 50 itérations des valeurs.

Afin de se familiariser avec l'utilisation de l'outil ainsi que les seuils associés aux valeurs à surveiller, rendez-vous sur http://www.yellow-bricks.com, le blog de Duncan Epping, et plus précisément la partie ESXTOP (mise à jour pour prendre en compte vSphere 6.5) : http://www.yellow-bricks.com/esxtop/

3. Outils externes

a. VMware vRealize Operations

vRealize Operations est une suite de produits. Selon la licence, les composants suivants sont disponibles :

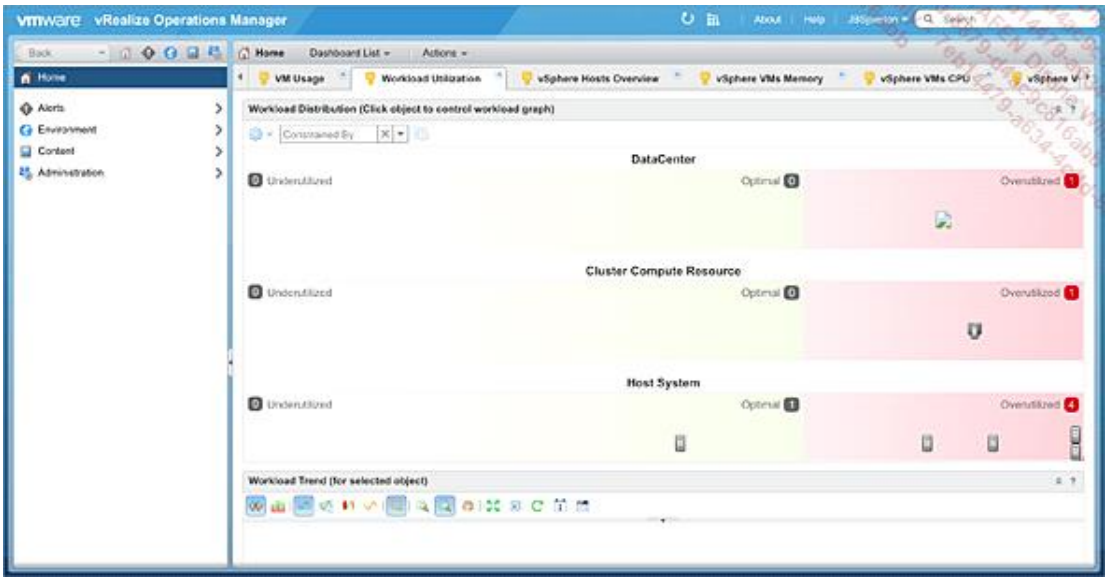
- vRealize Operations (vROps)
- vRealize Configuration manager (vCm)
- vRealize Hyperic
- vRealize Infrastructure Navigator

VMware vROps, anciennement vCenter Operations Manager permet la supervision de l'environnement virtualisé VMware ainsi que les baies de stockages et équipements réseau via des paquetages de gestion (*management packspp Packs*) disponibles sur VMware Solution Exchange. On y trouve des packs pour vSAN, NSX, Log Insight, les baies de stockage NetApp, les bases de données PostgreSQL, etc. (https://solutionexchange.vmware.com/store/category_groups/cloud-management?category=cloud-operations&nanosite_id=3&cloud_operations_ids[]=25&cloud_operations_ids[]=195&cloud_operations_ids[]=79&q=).

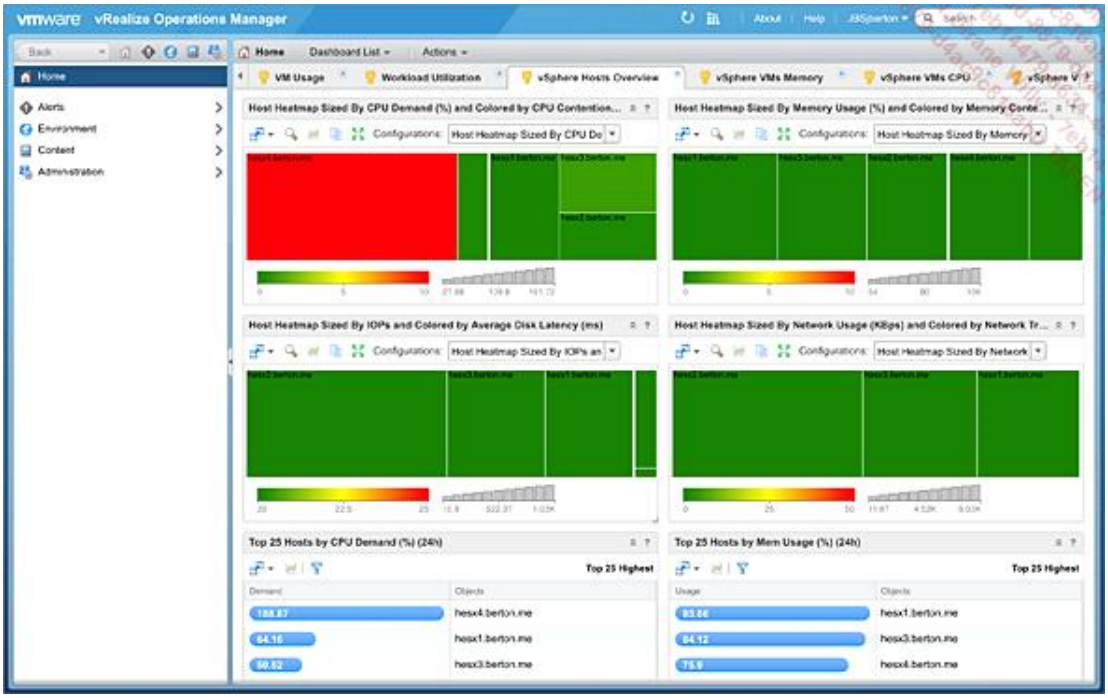
vROps permet d'optimiser l'utilisation des ressources, d'effectuer des prévisions (capacity planning) et de faire des simulations (scénarios « what-if).

Voici quelques exemples des tableaux de bord proposés par cet outil par défaut :

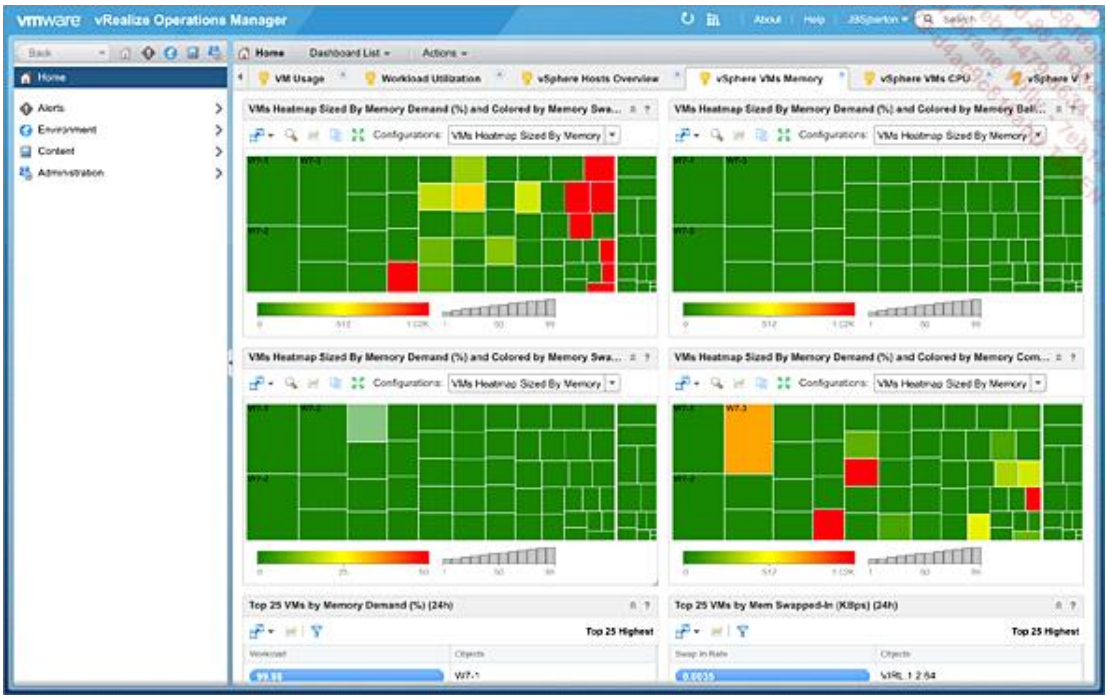
Analyse de répartition de charge



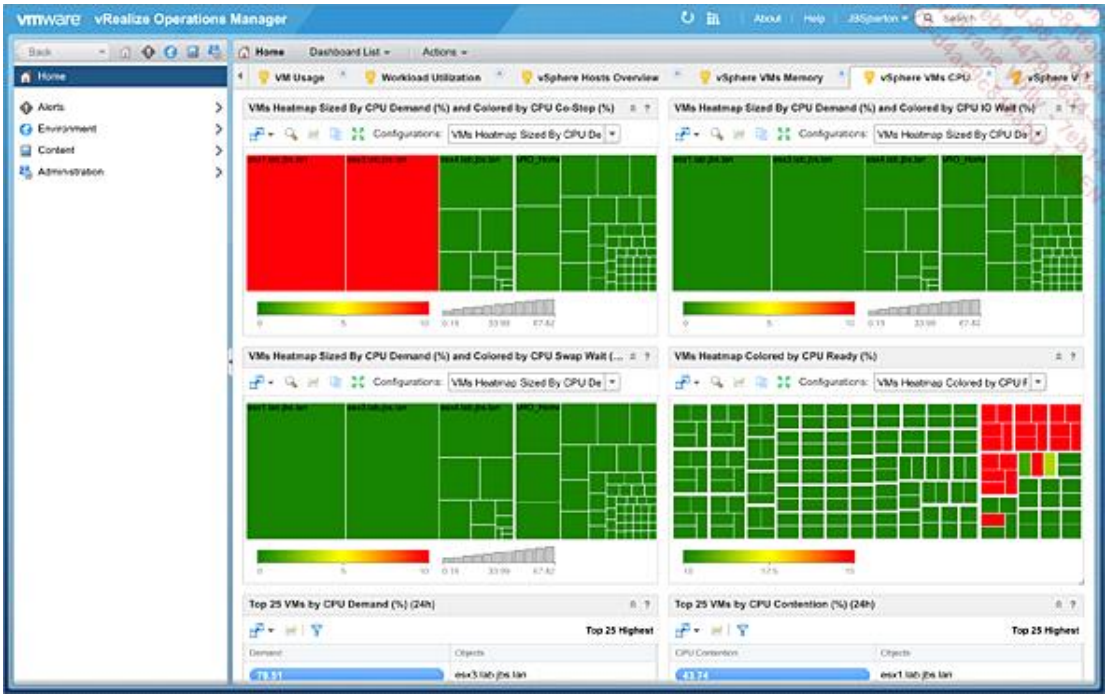
Analyse de l'utilisation processeur et mémoire des hôtes



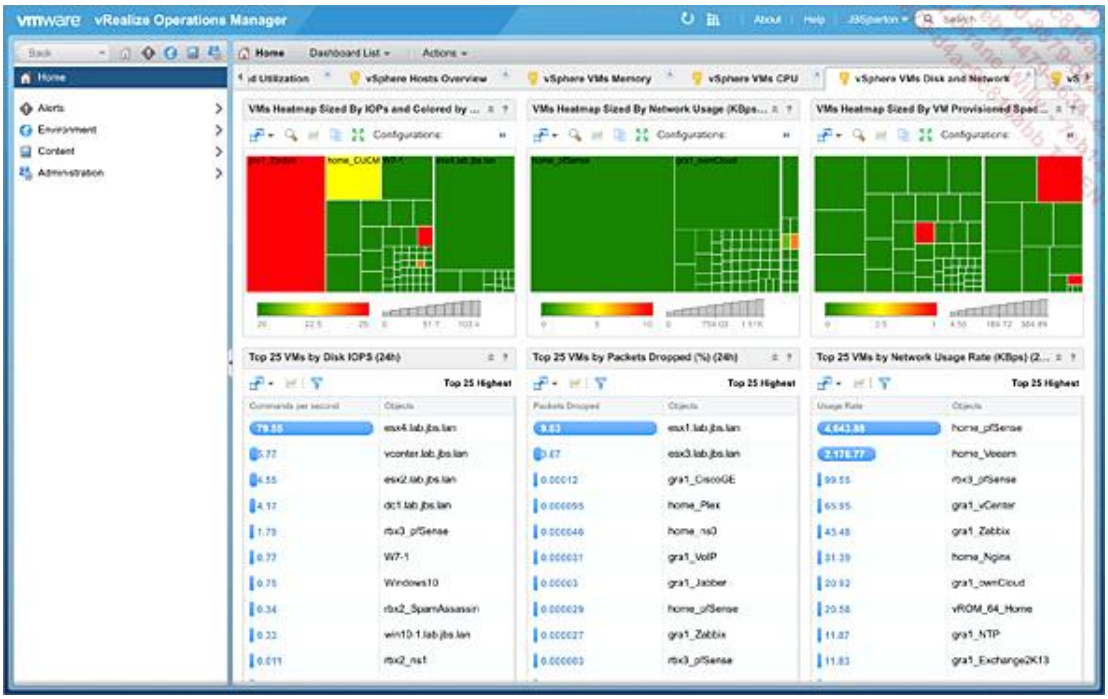
Consommation mémoire des machines virtuelles



Consommation processeur des machines virtuelles



Consommation disque et réseau des machines virtuelles



vRealize Configuration Manager permet la gestion d'une base de configuration centralisée des environnements physiques et virtuels. Configuration manager permet aussi la gestion de la conformité avec les normes et frameworks tels que PCI-DSS et SOX.

vRealizer Hyperic permet la surveillance des systèmes d'exploitation et des applications.

vRealize Infrastructure Navigator permet de chercher et d'afficher les dépendances entre différents composants et applications. Utilisé avec Site Recovery Manager, il permet d'indiquer à l'administrateur si des applications multitiers sont protégées en cas de défaillance d'un site dans le cadre du plan de reprise d'activité.

Pour plus d'informations, consultez le site de vRealize Operations : https://www.vmware.com/fr/products/vrealize-operations

b. VMTurbo Operations Manager

VMTurbo Operations Manager permet de surveiller les environnements VMware vSphere, Red Hat Enterprise Virtualization, Xenserver et Microsoft Hyper-V. Les fonctions sont similaires à vRealize Operations (supervision, optimisation et capacity planning). VMTurbo propose une licence gratuite du produit qui permet l'observation et l'envoi de rapports périodiques : VMTurbo Health monitor : http://vmturbo.com/downloads/vmturbo-virtual-health-monitor/

Tout comme vRealize Operations, il s'agit d'appliance virtuelle déployée en moins de 20 minutes.

VMTurbo s'appelle depuis octobre 2016 « Turbonomic ».