(https://pandorafms.com/blog/fr/)

COMMUNAUTÉ (HTTPS://PANDORAFMS.COM/BLOG/FR/CATEGORY/COMMUNAUTE/)
COMUNIDAD (HTTPS://PANDORAFMS.COM/BLOG/FR/CATEGORY/COMUNIDAD-PANDORAFMS-FR/)
RÉSEAUX (HTTPS://PANDORAFMS.COM/BLOG/FR/CATEGORY/RESEAUX/)
TECHNOLOGIE (HTTPS://PANDORAFMS.COM/BLOG/FR/CATEGORY/TECHNOLOGIE/)

Commandes réseau sous Windows et Linux

décembre 31, 2018

This post is also available in : Anglais (https://pandorafms.com/blog/network-commands/), Espagnol (https://pandorafms.com/blog/es/comandos-de-red/)

Commandes réseau fondamentales que tout administrateur devrait connaître

Dans cet article, nous allons vous montrer des différentes commandes réseau sous Windows et Linux qui sont indispensables pour tout administrateur réseau. On peut utiliser ces commandes réseau séparément ou combinées avec Pandora FMS (https://pandorafms.com/fr/), pour une surveillance en temps réel, ou comme partie d'une stratégie à long terme. Ce poste qui montre quelques outils réseau (https://blog.pandorafms.org/network-tools/) vous permettra mieux gérer vos réseaux et votre temps.

Si vous ne connaissez pas encore Pandora FMS, nous vous invitons à visiter notre site Web. Mais si vous êtes déjà familiarisé avec cet outil, vous saurez qu'il se distingue par sa flexibilité. Ce n'est pas surprenant donc, qu'il permette de personnaliser et créer des plugins surveillance. Avec ces commandes que nous allons aborder aujourd'hui, vous pourrez créer des plugins qui vous faciliteront beaucoup votre travail, en adaptant cet outil à vos besoins.

(https://bit.ly/2UwQWTD)

(https://bit.ly/2UwQWTD)

(https://bit.ly/2UwQWTD)

VNStat

C'est une des commandes réseau plus complètes. Elle fonctionne sous tous les systèmes Linux et BSD, et celle-là vous permet de surveiller le trafic réseau á partir de votre console.

- L'installation est très simple et assez rapide, en permettant la surveillance de toutes les interfaces réseau.
- Avec VNStat, vous pouvez recueillir tout le trafic dont vous avez besoin de, á partir de n'importe quelle interface configurée.
- L'une des grandes différences entre VNStat et d'autres outils c'est que VNStat cueille des données du noyau au lieu de l'interface elle-même, ce qui permet une exécution plus légère pour le système.
- Vous n'aurez pas besoin des autorisations d'administrateur pour l'exécuter.
- VNStat a la capacité de stocker l'information recueillie afin de ne pas perdre cette information, même si le système est bloqué ou redémarré.
- Vous avez la possibilité de configurer VNStat pour qu'il entende le trafic quotidiennement, à chaque période de facturation ou selon la fréquence que vous désirez.
- On met l'accent sur sa souplesse lors de la configuration de la lecture du trafic.
- Finalement, on peut mentionner que vous pouvez configurer la sortie de VNStat pour qu'il génère des graphiques par console et même les personnaliser avec des couleurs.

Ping (Unix/Windows)

Ping date des années 1970 et elle est connue pour être une des plus élémentaires commandes réseau. Cependant, elle n'est pas aussi simple que vous pouvez y croire et elle a beaucoup plus d'utilisations que ceux qu'on connait déjà. Elle est basé sur le protocole ICMP et sert à :

- Déterminer s'il y a une connectivité entre votre machine et une autre machine du réseau.
- Mesurer la « vitesse » ou le temps de latence.

```
En faisant un ping sur Wikipedia.org [91.198.174.192] avec 32 octets de données :
Réponse depuis 91.198.174.192 : bytes=32 temps=60ms TTL=54
Réponse depuis 91.198.174.192 : bytes=32 temps=50ms TTL=54
Réponse depuis 91.198.174.192 : bytes=32 temps=56ms TTL=54
Réponse depuis 91.198.174.192 : bytes=32 temps=50ms TTL=54

Statistiques de ping pour 91.198.174.192 :
      Paquets : envoyés = 4, reçus = 4, perdus = 0
      (0% perdus),
Temps approximatif d'aller-retour en millisecondes :
Minimal = 50ms, Maximal = 60ms, Moyenne= 54ms
```

Celles sont des commandes qui existent sous tous les systèmes d'exploitation qui supportent TCP/IP et ceux sont des éléments essentiels que vous devez connaître.

Ping se démarque par ses dizaines de paramètres et, ce qu'on trouve le plus utile c'est **qu'elle prend charge de la surveillance du « nombre de paquets à envoyer »**. Il y a des réseaux qui défont le premier paquet, donc il est indispensable d'envoyer au moins trois et être capable de vérifier qu'un d'entre eux est arrivé sans être écartée. **Pour cela, on peut utiliser le paramètre -c.**

Cette même technique permet de connaître le pourcentage de perte de paquets présent sur notre réseau, en envoyant dix paquets et en vérifiant si quelque d'entre eux est perdu. Certainement vous serez surpris du nombre de paquets perdus régulièrement sur le réseau. (Cet outil est intégré par défaut dans Pandora FMS).

Exécution : ping nom/IP d'équipe

Traceroute (Unix/Windows)

Cet outil a pour objectif principal de montrer la route qui parcourt un paquet par notre réseau. **Cette commande réseau vous permettra de savoir par où passe votre paquet (les machines, les switches, les routeurs) et vérifier que votre réseau fonctionne correctement.** Si elle détecte quelque problème, elle va vous permettre d'avoir une idée approximative sur où se trouve l'erreur.

Pandora FMS l'utilise dans son outil de mappage réseau (Recon Server) et grâce à cela, ainsi que d'autres outils avancés, il est possible de « dessiner » une hiérarchie du réseau.

```
Sur un maximum de 30 sauts :
1     6ms   1ms   2ms   192.168.1.1
2     5ms   5ms   4ms   192.168.144.1
3     9ms   5ms   5ms   101.red-81-46-10.customer.static.ccgg.telefonica.net [81.46.10.101]
4     6ms   6ms   17ms  110.red-81-46-8.customer.static.ccgg.telefonica.net [81.46.8.110]
5     6ms   11ms  8ms   interoute.baja.espanix.net [193.149.1.42]
6     6ms   5ms   11ms  ae0-0.mad-001-score-2-re0.interoute.net [89.202.161.18]
7     8ms   8ms   12ms  89.202.202.38
```

Exécution :
Traceroute – n (sous UNIX / Linux)
tracert – d (sous Windows)

Arp (Unix / Windows)

Cette commande réseau vous permet de modifier et afficher la table ARP, qui recueille les mappages entre l'adresse IP et l'adresse MAC. Mais elle n'examine que les connexions dans votre segment de réseau local (LAN), pourtant on pourrait l'appeler « de faible niveau ». Toutefois, elle sert à découvrir quelles sont les machines qui ont été directement reliées à notre hôte ou quelles sont lesquelles on a branché nous-mêmes. C'est un outil de diagnostic, et parfois il peut être convenable le surveiller afin d'écarter des attaques ARP Poisoning qui sont une des formes plus courantes d'attaque d'usurpation d'identité sur les réseaux locaux.

Dans Pandora FMS, une intégration habituelle consiste en vérifier, chez certains hôtes, que la correspondance d'IP et MAC est toujours la même. Si elle change soudainement, c'est parce que quelque hôte sur le réseau est en train de se faire passer par un autre.

Execution: arp –a

Curl et wget (Unix/ Windows)

Celles sont commandes indispensables pour faire des requêtes HTTP, HTTPS ou FTP aux serveurs à distance. Elles permettent de télécharger des fichiers ou des sites web entiers, même de manière récursive (ce qui nous permet de créer une « copie » littérale d'un site Web, compris ses images). Elles supportent des cookies et permettent d'envoyer des requêtes POST, en plus de pouvoir « simuler » un agent utilisateur et utiliser un proxy HTTP ou un proxy SOCKS4 / 5.

Une des utilités plus courantes en matière d'intégration avec Pandora FMS, c'est la vérification du contenu d'un site Web particulier. Comme wget et curl vous permettent de télécharger tout le contenu complet d'un site Web, il est facile de comparer le MD5 de ce contenu avec une valeur déjà vérifiée. Si cette valeur change, ça veut dire que le site Web a été modifié.

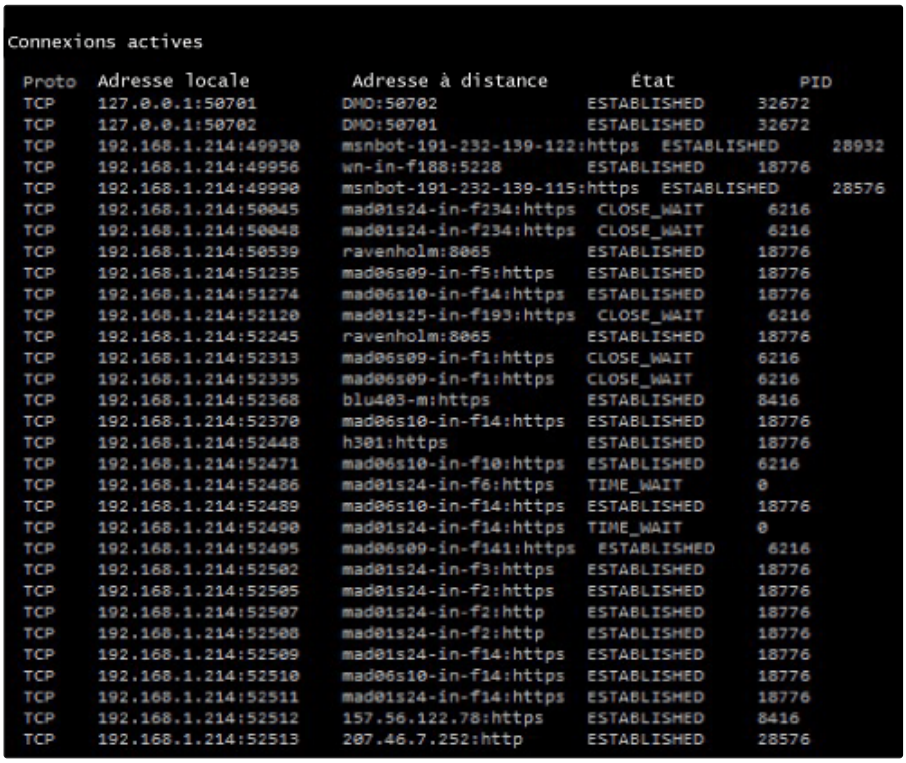
Netstat (Unix/Windows)

Une commande réseau qui identifie toutes les connexions TCP et UDP ouvertes dans un ordinateur. En outre, cela vous permet de connaître les informations suivantes :

- Tableaux de chemins pour connaître vos interfaces réseau et les sorties de celles dernières.
- Statistiques Ethernet qui vous montrent les paquets envoyés, ceux qui ont été reçus et aussi des possibles erreurs.
- Afficher le ID du processus qui est en train d'être utilisé par la connexion.

Netstat est une autre commande de base comme Ping qui remplit beaucoup de fonctions élémentaires. **Certains des éléments utilisés par les agents de Pandora FMS, pour obtenir des informations du système, sont les statistiques du trafic, le nombre de connexions ouvertes et le plus important, le**

nombre de connexions en suspens de fermeture ou en cours d'établissement. Une croissance inhabituelle de ces mesures peut devenir un problème sérieux et peut être dû à un problème de performance de votre serveur ou une attaque externe.



```
Connexions actives

  Proto  Adresse locale         Adresse à distance       État           PID
  TCP    127.0.0.1:50701        DMO:50702              ESTABLISHED     32672
  TCP    127.0.0.1:50702        DMO:50701              ESTABLISHED     32672
  TCP    192.168.1.214:49930    msnbot-191-232-139-122:https  ESTABLISHED     28932
  TCP    192.168.1.214:49956    wn-in-f188:5228        ESTABLISHED     18776
  TCP    192.168.1.214:49990    msnbot-191-232-139-115:https  ESTABLISHED     28576
  TCP    192.168.1.214:50045    mad01s24-in-f234:https  CLOSE_WAIT      6216
  TCP    192.168.1.214:50048    mad01s24-in-f234:https  CLOSE_WAIT      6216
  TCP    192.168.1.214:50539    ravenholm:8065         ESTABLISHED     18776
  TCP    192.168.1.214:51235    mad06s09-in-f5:https   ESTABLISHED     18776
  TCP    192.168.1.214:51274    mad06s10-in-f14:https  ESTABLISHED     18776
  TCP    192.168.1.214:52120    mad01s25-in-f193:https  CLOSE_WAIT      6216
  TCP    192.168.1.214:52245    ravenholm:8065         ESTABLISHED     18776
  TCP    192.168.1.214:52313    mad06s09-in-f1:https   CLOSE_WAIT      6216
  TCP    192.168.1.214:52335    mad06s09-in-f1:https   CLOSE_WAIT      6216
  TCP    192.168.1.214:52368    blu403-m:https         ESTABLISHED     8416
  TCP    192.168.1.214:52370    mad06s10-in-f14:https  ESTABLISHED     18776
  TCP    192.168.1.214:52448    h301:https             ESTABLISHED     18776
  TCP    192.168.1.214:52471    mad06s10-in-f10:https  ESTABLISHED     6216
  TCP    192.168.1.214:52486    mad01s24-in-f6:https   TIME_WAIT       0
  TCP    192.168.1.214:52489    mad06s10-in-f14:https  ESTABLISHED     18776
  TCP    192.168.1.214:52490    mad01s24-in-f14:https  TIME_WAIT       0
  TCP    192.168.1.214:52495    mad06s09-in-f141:https  ESTABLISHED     6216
  TCP    192.168.1.214:52502    mad01s24-in-f3:https   ESTABLISHED     18776
  TCP    192.168.1.214:52505    mad01s24-in-f2:https   ESTABLISHED     18776
  TCP    192.168.1.214:52507    mad01s24-in-f2:http    ESTABLISHED     18776
  TCP    192.168.1.214:52508    mad01s24-in-f2:http    ESTABLISHED     18776
  TCP    192.168.1.214:52509    mad01s24-in-f14:https  ESTABLISHED     18776
  TCP    192.168.1.214:52510    mad06s10-in-f14:https  ESTABLISHED     18776
  TCP    192.168.1.214:52511    mad01s24-in-f14:https  ESTABLISHED     18776
  TCP    192.168.1.214:52512    157.56.122.78:https    ESTABLISHED     8416
  TCP    192.168.1.214:52513    207.46.7.252:http      ESTABLISHED     28576
```

Whois (Unix / Windows)

Cette commande réseau est utilisée pour consulter des données sur des domaines, comme par exemple vérifier qui est le propriétaire du domaine ou quelle est la date d'expiration du domaine, et afficher les enregistrements configurés, les coordonnées, etc. Son utilisation est fortement recommandée pour contacter les administrateurs des domaines ou affronter des incidences des services tels que la migration web et mail.

Pour utiliser « whois » sous Windows, il faut télécharger le logiciel depuis **cette URL** (https://technet.microsoft.com/en-us/sysinternals/whois.aspx).

SSH (Unix / Linux / Windows)

Une commande pour exécuter des terminaux sur des équipements à distance en toute sécurité. SSH permet à tout utilisateur d'exécuter une console tout simplement en enregistrant et en entrant ses identifiants. Ainsi, vous pouvez exécuter les commandes que vous voulez comme si vous étiez sur place.

Plus de détails que vous devez savoir sur SSH :

- **Pour utiliser SSH sous Windows, Putty est recommandé.** Vous pouvez le trouver **à l'adresse (http://www.putty.org/)**

- Pour permettre qu'un équipement à distance puisse se connecter à votre serveur via SSH, **vous devez installer et configurer un serveur SSH comme FreeSSHd.**

- SSH permet en outre d'obtenir un Shell distant interactif, exécuter des commandes à distance et copier des fichiers dans les deux sens.

- Il ne faut pas oublier que SSH est le remplacement naturel des outils tels que Telnet ou FTP, et qu'il est devenu au fil des années l'outil fondamental de gestion des systèmes. Il est extrêmement puissant, et malgré ses combinaisons complexes de chiffrement symétrique et ses schémas d'authentification et de vérification, c'est la cible d'attaques incessantes.

Pandora FMS utilise SSH de différentes manières et vous donne la possibilité d'exécuter des commandes à distance. Pour des raisons de sécurité, l'utilisateur doit établir un schéma d'authentification sur base des certificats, ce qui permet d'établir des connexions d'exécution à distance à partir d'une machine sans demander aucun mot de passe. C'est convenable, mais légèrement complexe à mettre en place. Par conséquent, sous la version Entreprise, notre serveur Satellite permet plusieurs exécutions à distance sur différents hôtes d'une manière beaucoup plus optimisée et simple. Ça nous permet de faire des centaines de contrôles par seconde.

TCPDump (Unix/Linux/Windows)

C'est un autre des outils « fondamentales » en matière de commandes réseau, qui peut devenir un grand allié pour les administrateurs réseau, administrateurs système ou programmeurs, s'ils l'utilisent correctement.

TCPDump est une commande avancée utilisée pour inspecter le trafic des différentes interfaces d'une machine et d'obtenir ainsi les paquets échangés. Vous pouvez verser au fichier la sortie, puis l'analyser avec d'autres renifleurs plus puissants et avec des interfaces graphiques telles que **Wireshark (https://www.wireshark.org/)**. Sous Windows, utilisez **WinDump (https://www.winpcap.org/windump/)**.

Ngrep (Unix/Linux/Windows)

- Il emporte la puissance de la commande grep au réseau.

- C'est comme TCPDump mais avec un filtre de sous-chaînes de caractères en temps réel.

- Il a un système de filtrage des expressions régulières très puissant et il est généralement utilisée pour traiter les fichiers générés par TCPDump, Wireshark, etc.

- C'est un filtre de paquets de communications sur des protocoles http, SMTP, FTP, DNS et d'autres.

NMAP (Unix/Windows)

NMAP est considéré comme le père des scanners réseau générales. Quoique aujourd'hui il y a des outils plus fiables pour certaines tâches (par exemple : Fping), NMAP est un outil polyvalent pour le scannage des réseaux. Il sert à déterminer quels hôtes sont actifs dans un réseau et faire des analyses des différents manières.

Netcat (Windows/Unix)

NetCat, ou NC, est la commande réseau plus polyvalente qui existe et l'une des plus légères. Toutefois, son utilisation exige un peu d'imagination. Seulement si vous avez bidouillé avec des scripts, vous comprendrez la subtilité de son nom : NetCat. C'est un outil destiné à être utilisé comme destination d'une redirection (un pipe ou |). Elle sert à envoyer ou recevoir des informations d'une connexion. Par exemple, une requête Web à certain service serait quelque chose d'aussi simple que :

```
echo -e "GET http://pandorafms.com HTTP/1.0\n\n" | nc pandorafms.com 80
```

Lsof (Unix/Windows)

La commande « lsof » n'est pas seulement utilisée comme outil réseau, mais elle aussi sert à déterminer quels fichiers ont un processus ouvert. Dans des environnements Unix, un fichier peut être une connexion réseau, donc c'est utile pour savoir quels sont les ports ouverts d'un processus particulier en cours d'exécution, ce qui peut être très utile selon les cas.

Également, on peut l'utiliser pour savoir combien de fichiers sont ouverts dans un processus. Ça n'a rien à voir avec le réseau, mais sûrement ça peut être utile.

IPtraf (Linux)

Commande spécialisée pour obtenir des statistiques de trafic. Elle a une interface ncurses (texte) pour analyser le trafic qui passe par une interface en temps réel. Cela permet de travailler en performance réduite et voir quelles sont les paires de connexions établies dans chaque machine, en affichant en détail le trafic par paire de connexion, tout en temps réel. Très utile si vous détectez quelque chose d'étrange sur votre machine et vous ne savez pas quel trafic la traverse.

On espère que vous ayez trouvé intéressant cette liste de commandes réseau. Est-ce qu'on a oublié certaine commande réseau? N'hésitez pas à nous dire afin de l'inclure dans cette liste.

À propos de Pandora FMS

Pandora FMS est un **logiciel de supervision flexible**, capable de surveiller **des appareils, des infrastructures, des applications, des services et des processus d'entreprise**.

Voulez-vous savoir ce que Pandora FMS peut vous offrir ? Pour en savoir plus : https://pandorafms.com/fr (https://pandorafms.com/fr)

Ou si vous avez à surveiller plus de 100 appareils, vous pouvez également profiter d'un **ESSAI GRATUITE** de 30 jours de Pandora FMS Enterprise. Obtenez-le ici (https://pandorafms.com/fr/essai-gratuit/?utm_source=blog&utm_medium=democol&utm_campaign=blog_ene2020_en).

Par ailleurs, n'oubliez pas que si vos besoins en matière de supervision sont plus limités, vous avez à votre disposition la version OpenSource de Pandora FMS. Pour plus d'informations, voir : https://pandorafms.org/ (https://pandorafms.org/)

N'hésitez pas à envoyer vos questions, **l'équipe de Pandora FMS se fera un plaisir de vous aider !**

WRITTEN BY:
LAURA CANO (HTTPS://PANDORAFMS.COM/BLOG/FR/AUTHOR/LAURA-CANO/)

previous post

erte de paquets : les problèmes, les causes et les solutions s://pandorafms.com/blog/fr/perte-de-paquets/)

(https://pandorafms.com/blog/fr/outils-systeme/)

(https://pandorafms.com/de-paquets/)

next post

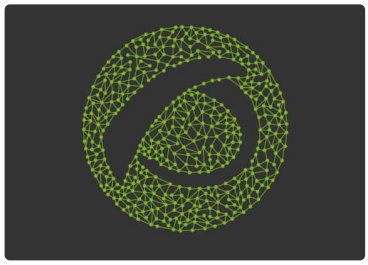
Des outils système : tous les outils qu'un administrateur Windows doit connaître (https://pandorafms.com/blog/fr/ou systeme/)

You may also like..

(https://pandorafms.com/blog/fr/quest-ce-que-netflow/)

Qu'est-ce que NetFlow ? Profitez-en et découvrez-le une fois pour toutes ! (https://pandorafms.com/blog/fr/quest-ce-que-netflow/)

février 4, 2020



(https://pandorafms.com/blog/fr/feuille-de-route-pandora-fms-2020-2021/)

L'avenir de Pandora FMS: feuille de route 2020-2021 (https://pandorafms.com/blog/fr/feuille-de-route-pandora-fms-2020-2021/)

décembre 3, 2019

(https://pandorafms.com/blog/fr/logiciel-rolling-release/)

Si vous recherchez des résultats différents, ne faites pas toujours la même chose, développez des logiciels hétérodoxes! (https://pandorafms.com/blog/fr/logiciel-rolling-release/)

septembre 18, 2019

(https://pandorafms.com/blog/fr/bases-de-donnees-nosql/)

Bases de données NoSQL : Le guide définitif (https://pandorafms.com/blog/fr/bases-de-donnees-nosql/)

juin 25, 2019

LEAVE A COMMENT

Your comment here..

Name

E-mail

URL (optional)

Enregistrer mon nom, mon e-mail et mon site web dans le navigateur pour mon prochain commentaire.

Laisser un commentaire

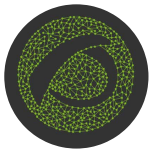
février 4, 2020

Qu'est-ce que NetFlow ? Profitez-en et découvrez-le une fois pour toutes ! (https://pandorafms.com/blog/fr/quest-ce-que-netflow/)

(https://pandorafms.com/blog/fr/quest-ce-que-netflow/)

décembre 3, 2019

L'avenir de Pandora FMS: feuille de route 2020-2021 (https://pandorafms.com/blog/fr/feuille-de-route-pandora-fms-2020-2021/)



(https://pandorafms.com/blog/fr/feuille-de-route-pandora-fms-2020-2021/)

septembre 18, 2019

Si vous recherchez des résultats différents, ne faites pas toujours la même chose, développez des logiciels hétérodoxes! (https://pandorafms.com/blog/fr/logiciel-rolling-release/)

(https://pandorafms.com/blog/fr/logiciel-rolling-release/)

CATÉGORIES

Communauté (19) (https://pandorafms.com/blog/fr/category/communaute/) Comunidad (13) (https://pandorafms.com/blog/fr/category/comunidad-pandorafms-fr/) Culture geek (4) (https://pandorafms.com/blog/fr/category/culture-geek/) Enterprise (4) (https://pandorafms.com/blog/fr/category/enterprise-fr/) Featured (3)

(https://pandorafms.com/blog/fr/category/featured-fr/) Fonctionnalités (5)
(https://pandorafms.com/blog/fr/category/fonctionnalites-fr/) Funcionalidades (2)
(https://pandorafms.com/blog/fr/category/funcionalidades-pandorafms-fr/) Nouage et Virtualisation (1)
(https://pandorafms.com/blog/fr/category/nouage-et-virtualisation/) Progiciel (8)
(https://pandorafms.com/blog/fr/category/progiciel/) Réseaux (3)
(https://pandorafms.com/blog/fr/category/reseaux/) Serveurs (2)
(https://pandorafms.com/blog/fr/category/serveurs/) Tech (6)
(https://pandorafms.com/blog/fr/category/tech-pandorafms-fr/) Technologie (13) (https://pandorafms.com/blog/fr/category/technologie/)

(https://twitter.com/pandorafms) (https://www.facebook.com/pandorafms) (https://www.linkedin.com/company/2720642/) (https://www.youtube.com/user/PandoraF