Debian GNU/Linux

Maîtrisez la sécurité des infrastructures

informatique technique

Fichiers complémentaires
à télécharger

Collection EPSILON

Philippe PIERRE

Table des matières

Les éléments à télécharger sont disponibles à l'adresse suivante :
http://www.editions-eni.fr
Saisissez la référence ENI de l'ouvrage **EPSIDEB** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Avant-propos

Chapitre 1
Outils de sauvegarde

Chapitre 2
Outils d'audit et d'analyse

Chapitre 3
Outils de surveillance et supervision

Chapitre 4
Services système et administration

Chapitre 5
De la redondance au cluster

Chapitre 6
Loadbalancing et qualité de service

Chapitre 7
Outils forensic

Conclusion

Chapitre 3
Outils de surveillance et supervision

1. Surveillance basique

1.1 Présentation et définitions

Après s'être intéressé à l'analyse des différentes machines d'une infrastructure, il est temps d'étudier la mise en place d'instruments de supervision sur les machines de l'environnement de production. Avant de commencer, il est important de bien distinguer l'analyse et la supervision. Dans le premier cas, comme abordé dans le chapitre précédent, il s'agit plus de récupérer de l'information, ponctuellement. Alors que dans le cas présent nous chercherons à garder un œil (voire les deux, de préférence) sur l'évolution de l'exploitation des machines du parc informatique. La définition exacte de la supervision informatique est la suivante : il s'agit de la surveillance du bon fonctionnement d'un système et/ou d'une activité. C'est pourquoi il est primordial de posséder un mécanisme connecté en permanence, remontant les alertes en cas d'incidents. Cela doit permettre de rapporter, alerter et surveiller les fonctionnements aussi bien normaux qu'anormaux des systèmes informatiques. Cette préoccupation doit répondre aux points suivants :

- surveillance technique : gestion du réseau, de l'infrastructure et des machines sous-jacentes
- surveillance applicative : gestion des applications et des processus métiers
- surveillance des contrats de services : gestion des indicateurs contractuels, type SLA
- surveillance métier : inspection des processus métiers de l'entreprise via des KPI

Dans ce dernier cas, nous devons bien sûr nous assurer que l'ensemble des fonctionnalités mises en œuvre par les informaticiens respecte bien les préoccupations du cœur de métier. En d'autres termes, l'informatique n'est que l'outil permettant d'aider l'entreprise à être plus rentable et plus réactive. Le système de supervision est là pour envoyer des messages sur la console, aux administrateurs et aux utilisateurs, en cas de dysfonctionnement. Ce genre d'activité doit se faire après avoir sécurisé l'écosystème et de façon systématique 24h/24, 7j/7. Plusieurs méthodes de supervision sont à distinguer :

– la méthode locale, à l'aide d'outils spécialisés
– la méthode externe type ASP (***A****pplication* ***S****ervice* ***P****rovider*), au travers d'Internet
– la méthode SaaS (***S****oftware* ***a****s* ***a*** ***S****ervice*) via un Cloud privé ou hybride

Ces deux dernières techniques permettent à l'utilisateur :

– d'éviter les intégrations d'infrastructures techniques.
– de pouvoir se passer de compétences spécifiques dédiées au fonctionnement de ces solutions.
– d'éviter un investissement dans un logiciel particulier, spécialisé.
– de disposer d'une solution simple, même avec une informatique répartie géographiquement.
– de consulter n'importe où et à tout moment les données collectées.

La seule contrainte de ce genre de solution est la forte dépendance à un fournisseur d'accès à Internet ou prestataire de Cloud. En fait, le choix de la solution dépend fortement du besoin et des contraintes imposées par les utilisateurs. Dans le cas le plus simple, après avoir correctement sécurisé l'ensemble des couches du système d'exploitation Linux Debian, l'étape suivante consiste à s'intéresser à la détection d'incidents (de préférence avant l'utilisateur), voire même d'anticiper les pannes en s'appuyant alors sur la supervision du système. Mais, outre les méthodes évoquées précédemment, il existe différents niveaux de supervision :

La supervision locale

Pour certaines entités, relativement petites, il est quelquefois plus intéressant de gérer les différents aspects de la supervision, en local : c'est-à-dire, sur chaque serveur du réseau. Cela permet d'avoir individuellement un tableau de bord pour chaque machine et de pouvoir valider tous les échelons : système, réseau, performances disques, ressources mémoire... et également de valider les éventuels goulots d'étranglement de façon rapide. Cela s'apparente à un mode dit "dashboard" dans lequel nous pourrons utiliser indifféremment :

– `Glances`
– `lynis`

La gestion des métriques du système

Dans le cadre de clusters de calculs ou de groupements de machines plus importantes, nous pouvons aussi nous intéresser uniquement à l'aspect système en remontant essentiellement les métriques telles que CPU, performances disques, utilisation de la mémoire, occupation disques... mais sans pour autant nous préoccuper du réseau et de l'environnement extérieur (même si celui-ci reste indéfectiblement lié à la machine). Ainsi, nous pouvons facilement déterminer les points d'amélioration d'un serveur et prédire ses défaillances. Cela correspond plus à un mode de supervision système qui pourra être géré par :

– `ganglia`

– `cacti`

La supervision avec gestion d'état

Au sein d'infrastructures assez conséquentes, la supervision devient plus délicate et nécessite très souvent de pouvoir constituer des rapports généraux, mais également de zoomer spécifiquement sur certaines métriques au travers du temps afin de connaître les fréquences d'usure et d'utilisation des équipements. Cela correspond plus à un mode basique que pourront fournir :

– `zabbix`

– `munin`

La supervision orientée métier

Très rapidement, les informaticiens ont eu besoin d'orienter leur surveillance autour d'applications spécifiques et de les corréler à leurs équipements. C'est pourquoi certains logiciels s'articulent autour des préoccupations métier, plus proches des utilisateurs, comme les outils :

– `nagios`

– `centreon`

La supervision universelle modulaire

Étant donné que la préoccupation finale reste néanmoins l'utilisateur et ses applications, il a également fallu orienter la supervision universelle vers des aspects plus métiers que Nagios. C'est dans cette vision qu'est né `Shinken`.

Remarque

On pourra aussi détailler l'aspect analyse du trafic réseau permettant de vérifier les types de paquets transitant entre les différentes machines de l'entreprise, y compris ceux entrant ou sortant du LAN. De plus, il existe de nombreuses autres solutions commerciales telles que WhatsUpGold, ou encore PRTG.

La supervision industrielle

Il existe des solutions pour le contrôle de processus et d'automatisation. Ici, on s'intéresse uniquement à la partie spécifique du processus de supervision au sein d'un corps de métiers. En ce cas, seront utilisés des outils comme :

– `Proview` : pour le contrôle de processus et/ou d'automatisation
– `Lintouch` : pour la création des applications SCADA pour clients individuels
– `EnergoSCADA` : pour le contrôle de la supervision énergétique des bâtiments

1.2 Installation de Glances

Lorsqu'un serveur est mis en production au sein d'une petite entité, nous souhaiterons surveiller a minima l'utilisation des ressources de celui-ci : RAM, CPU, disques... Pour cela, nous installerons un utilitaire, appelé `Glances` sur le serveur en question. Il s'agit d'un programme développé en Python par Nicolas HENNION, effectuant une surveillance des serveurs en mode texte (comparable en cela à l'utilitaire `htop`, ou `pstree`). Cela signifie que pour l'installer, nous devrons passer par le gestionnaire d'installation Python officiel, appelé `pip` :

```
# apt-get install python-dev python-pip
```

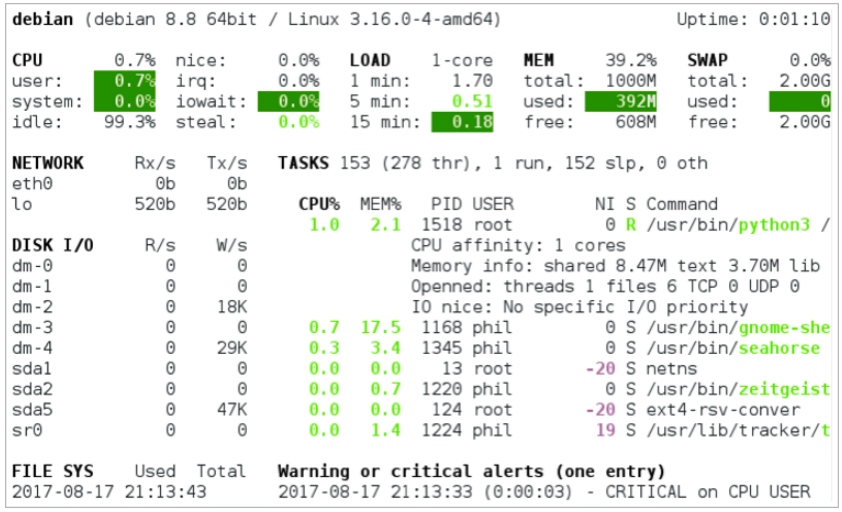
Remarque

Depuis la version Debian 8 (Jessie), il existe un package `glances` installable directement, mais jusqu'à la version Wheezy, il est nécessaire de passer par l'assistant Python.

Il ne reste plus alors qu'à installer le programme `glances`, en installant le package éponyme :

```
# apt-get install glances
```

Invoquons la commande `glances` pour pouvoir vérifier le bon fonctionnement :



Remarque

Il arrive parfois que l'affichage se fasse sur un fond clair avec des caractères presque blancs. Pour optimiser l'affichage pour un fond blanc, il faut utiliser l'option `--theme-white`.

Comme nous le constatons sur cette capture, l'écran est alors fractionné en sept grandes familles permettant de disposer en un coup d'œil des principales métriques du système :

- `CPU`
- `LOAD`
- `MEM`
- `SWAP`
- `NETWORK`
- `TASKS`
- `DISK I/O`

La première ligne de l'écran contient à la fois le nom du serveur, sa distribution, ainsi que sa version et l'architecture du serveur. Les codes couleur parlent d'eux-mêmes :

- Le vert : pour signifier que la statistique est acceptable.
- Le bleu : pour signifier qu'il faut faire attention (à surveiller).
- Le violet : pour signifier que la statistique est en alerte.

– Le rouge : pour signifier que la statistique est critique.

Nous pouvons nous assurer de la bonne installation de l'outil en vérifiant la version de celui-ci :

```
root@debian:/home/phil# glances -V
Glances v2.1.1 with psutil v2.1.1
```

1.3 Modes d'utilisation

Suite à la demande de nombreuses personnes, Glances v2 intègre, en plus du mode "*standalone*" (permettant de superviser une machine localement), et de son mode client/serveur (option `-s`), permettant de surveiller n'importe quelle machine distante, un mode web. En lançant le programme en mode serveur web (c'est-à-dire en utilisant l'option `-w`), nous pouvons alors interroger l'application depuis n'importe quel navigateur web présent sur le système local ou distant. Ainsi, en ouvrant un navigateur web avec l'adresse http://localhost:61208 (ou http://debian.mydmn.org/61208), nous devrions alors pouvoir visualiser la même interface que précédemment, mais au travers du navigateur :