

Z-Eye, monitoring et gestion réseau unifiée

Loïc Blot

Institut Optique Graduate School
2 avenue Augustin Fresnel
91127 Palaiseau Cedex

Résumé

Z-Eye est une solution de monitoring et gestion réseau unifiée. Créée suite à un besoin de visibilité et de recoupement de données de monitoring, Z-Eye a évolué afin de permettre de centraliser l'information, la rendant plus précise, mais également de gérer certaines parties d'un réseau.

Z-Eye utilise les logiciels libres suivants (liste non exhaustive).

- *Netdisco*
- *MRTG*
- *Icinga*
- *Snort*
- *Barnyard2*
- *PostgreSQL 9.2*
- *Apache 2.4*

Z-Eye articule l'ensemble des informations de monitoring et de gestion au sein d'une interface web moderne et intuitive développée en PHP/AJAX et d'un service de collecte et gestion asynchrone développé en Python.

En terme de gestion réseau, Z-Eye permet de gérer des commutateurs Cisco (VLAN, CDP, 802.1x, descriptions), et certaines fonctions triviales de constructeurs comme Dell et HP. D'autres fonctionnalités permettent de gérer finement des ensembles de serveurs DHCP et DNS UNIX (ISC-dhcpd et named/Bind9) ou encore des bases de données de serveurs RADIUS (FreeRADIUS) et les différentes données d'accounting.

Afin de faciliter la visualisation de la sécurité au sein d'un réseau, le moteur Snort est présent, collectant les données sur une interface dédiée et avertissant de certains types de menaces. Icinga est quant à lui entièrement administrable et visualisable sur l'interface web de Z-Eye.

Enfin, l'outil de recherche permet de trouver rapidement toutes les correspondances d'un élément donné, que ce soit une adresse MAC, une adresse IP, un nom DNS ou encore un nom d'utilisateur et bien d'autres encore.

Mots-clefs

Monitoring, Réseau, DHCP, Commutateurs, DNS, RADIUS, IDS, Journaux

1 Introduction

Z-Eye est une distribution libre dont le but est de simplifier la gestion complète d'un réseau, par le recoupage d'informations, mais également de pouvoir administrer de manière intuitive et simple les différents composants de celui-ci. Z-Eye est une distribution basée sur FreeBSD 9.1.

2 Modèle de développement

Z-Eye repose sur un modèle à trois licences.

- Licence BSD pour sa librairie de développement PHP
- Licence GPLv2 pour son moteur
- CC-by-NC pour son design

Le modèle de développement de Z-Eye s'appuie sur le logiciel libre Git. Il existe 2 branches dans l'arbre officiel de la distribution.

- Stable : version de production destinée au public
- Current : version de développement

Le rythme de publication de nouvelles versions de Z-Eye ne dépend pas d'un calendrier fixe. En effet, une release est caractérisée par l'apparition de nouvelles fonctionnalités dans la version « current ». Une fois celle-ci stabilisée au terme d'un processus de tests d'environ un mois. Cette version est estampillée « stable ».

Des correctifs sont appliqués sur la dernière version stable sortie et peuvent être reportés sur d'anciennes versions dans le cas d'un support entreprise.

3 Fonctionnalités

3.1 Monitoring actif

L'utilisation du moteur Icinga et de sondes NRPE permet d'effectuer du monitoring actif, que ce soit sur des équipements réseau ou des serveurs.

L'interface web de Z-Eye permet de gérer directement l'ensemble de la configuration Icinga. [1]

3.2 Gestion de commutateurs

Z-Eye permet de récolter des informations sur énormément d'équipements réseau, grâce au back-end Netdisco. Si vous possédez des commutateurs de marque Cisco, il est également possible d'administrer les ports de ces commutateurs de manière très simple et d'apposer des données administratives (prise et pièce dans vos bâtiments). Z-Eye peut également lancer des sauvegardes automatisées de ces équipements. [2]

Lorsqu'un équipement est découvert ou ajouté à Z-Eye, un processus de collecte d'informations des débits par port est automatiquement lancé via MRTG. Ce processus permet également de générer des graphiques.

Le module de gestion de commutateurs utilise également un système de droits fins permettant de gérer des profils d'utilisateurs.

3.3 Gestionnaire IP

Le gestionnaire IP est apparu dans la version 1.2 de Z-Eye. Celui-ci permet de gérer de manière graphique et relationnelle un ou plusieurs serveurs DHCP, en mode seuls ou en clusters.

Il est ainsi possible de définir des réseaux IP, de réserver des adresses, d'ajouter des ranges et des options DHCP à

distribuer à vos clients sur le réseau. Cette fonctionnalité s'appuie sur une communication via SSH et écrit des fichiers de configurations plats sur vos serveurs UNIX. [3]

Il est également possible de définir des droits associés à vos profils d'utilisateurs.

3.4 Gestionnaire DNS

Dans la future version 1.3 de Z-Eye il sera possible de gérer vos serveurs DNS UNIX. Les anciennes versions de Z-Eye apportaient déjà la lecture des configurations et enregistrements.

La gestion DNS permettra de déclarer rapidement des noms de domaines DNS et leurs enregistrements, mais également de gérer les ACLs et certains aspects DNSSec.

3.5 Gestion RADIUS

Z-Eye intègre également un connecteur à une ou plusieurs bases de données de serveurs (Free)RADIUS (MySQL/PgSQL). Cela permet de gérer rapidement l'ensemble des utilisateurs, groupes et attributs RADIUS retournés par vos serveurs RADIUS. Cette fonction s'avère efficace dans le cas d'une authentification MAB (authentification 802.1x par adresse MAC). [4]

Il est possible de déléguer des droits sur un serveur RADIUS afin de créer des comptes en masse, utile dans le cas d'un portail captif pour vos invités.

Afin de purger les données utilisateur, la solution intègre également une notion d'expiration qui permettra de supprimer automatiquement les données obsolètes.

La version 1.3 de Z-Eye intégrera la possibilité de visualiser et analyser les différentes données d'accounting récoltées dans les différentes bases de données.

3.6 IDS/IPS Snort

Snort est intégré de manière triviale sur Z-Eye. En dédiant un port de commutateur relié au serveur Z-Eye et en effectuant un port mirroring, Snort pourra détecter les menaces en temps réel sur votre réseau.

3.7 Recherche

L'outil principal est la recherche. Z-Eye permet de rechercher rapidement dans l'ensemble des données collectées par toutes ses sondes et données renseignées par l'utilisateur. Il est ainsi très simple de retrouver où est connectée une adresse MAC, quelle est son adresse IP associée dans le DHCP, combien de données ont été consommées par un utilisateur et bien plus encore. [5]

3.8 Authentification

Z-Eye s'appuie sur une authentification par identifiant/mot de passe. Celle-ci s'appuie sur un ou plusieurs annuaires de type LDAP ou Active Directory. Le seul utilisateur local est le super-administrateur, possédant tous les droits.

3.9 Journaux

Z-Eye enregistre toute action de modification ou de recherche de la part de l'utilisateur. Cela permet de pouvoir identifier des problèmes a posteriori.

4 Retours d'expérience

Voici plusieurs retours d'expérience sur l'utilisation de Z-Eye par Gilbert Lucas, DSI de l'Institut Optique Graduate School, Laurent Leclercq, Administrateur systèmes et téléphonie et Jean-Philippe Morvan, Développeur à la mairie de Villejuif.

4.1 Gilbert Lucas, DSI de l'IOGS (Institut Optique Graduate School)

« L'installation de Z-Eye au sein du service informatique de l'IOGS a permis de faciliter la gestion de l'ensemble de nos équipements réseau (nous avons un parc homogène Cisco).

Désormais, nous utilisons cet outil au quotidien pour :

- modifier la configuration du port d'un commutateur (changement de vlan, ...), l'activer ou le mettre hors service ;*
- effectuer des recherches poussées, par numéro de prise, par pièce, par @ MAC ou @ IP ou par nom ;*
- enregistrer des machines par @ MAC dans le DHCP, déclarer des noms DNS ;*
- faire des statistiques d'utilisation, par exemple, pour l'occupation des zones DHCP ;*
- pouvoir superviser l'ensemble des services en ayant des remontées d'alertes en cas de dysfonctionnement ;*
- surveiller les tentatives d'intrusions.*

La prise en main de cet outil s'est faite facilement, car l'interface graphique est intuitive et à l'usage, il nous fait gagner énormément de temps. (et l'avantage d'avoir le développeur sous la main, c'est que l'on peut faire des demandes de correctifs facilement)

En conclusion, je recommande l'installation et l'usage de Z-Eye car c'est un outil libre et gratuit qui condense en un seul logiciel plusieurs autres à l'installation et à la configuration délicate. »

4.2 Laurent Leclercq, Administrateur systèmes et téléphonie à l'IOGS

« Z-eye est un outil facilitant la gestion au quotidien de l'infrastructure réseau.

Il est devenu incontournable la configuration rapide des commutateurs et dans la gestion au quotidien. »

4.3 Jean-Philippe Morvan, Développeur à la mairie de Villejuif

« Nous utilisons principalement la gestion des équipements réseau nous permettant ainsi d'avoir une vision globale de nos matériels actifs et de visualiser/modifier rapidement leur configuration en mode 'human-readable' et surtout avec peu de notions HP ou Cisco. A terme, nous souhaitons l'utiliser également en monitoring système. »

5 Conclusion

Z-Eye est un outil libre améliorant la productivité et la collecte d'informations. Il simplifie la tâche de ceux qui l'ont adopté en fournissant des informations précises et fiables, et permet de gérer de manière centralisée certains composants essentiels d'un réseau.

Z-Eye est pensé pour rester simple d'utilisation et faciliter l'administration de services sans avoir les connaissances techniques nécessaires. Le produit est en évolution permanente, intégrant de nouveaux services, modernisant l'expérience utilisateur et ajoutant de nouvelles fonctionnalités. La version 1.3 est d'ailleurs prévue pour le mois de décembre, ainsi qu'une application Android.

Il est très facile d'installer Z-Eye, l'installateur étant une version allégée de celui présent sur FreeBSD, suivi d'un accès direct à l'interface web qui accompagnera les nouveaux utilisateurs dans la finalisation de l'installation.

L'équipe de développement reste à l'écoute de la communauté, que ce soit pour l'ajout de nouvelles fonctionnalités, les suggestions d'améliorations ou encore la correction de bugs. Nous sommes aussi prêts à accueillir de nouveaux bras et de nouvelles idées.

L'essayer, c'est l'adopter.

Pour tout renseignement : contact at z-eye dot org

6 Références

- [1] Documentation Z-Eye, Icinga: http://z-eye.org/Configuration_du_moniteur_syst%C3%A8me
- [2] Documentation Z-Eye, Équipements réseau: http://z-eye.org/Gestion_des_%C3%A9quipements_r%C3%A9seau
- [3] Documentation Z-Eye, IPM: http://z-eye.org/Gestionnaire_IP
- [4] Documentation Z-Eye, RADIUS: http://z-eye.org/Gestion_d%27utilisateurs_et_groupes_FreeRadius2
- [5] Documentation Z-Eye, Recherche: <http://z-eye.org/Recherche>