Description de la prestation « Journalisation des requêtes DNS Windows »

Historique du document

Version	Modification	Date	Auteur
0.1	Premier brouillon	04 jan. 2012	Patrick Saladino (PS)
0.2	Ajout de la partie technique	05 jan. 2012	Patrick Saladino (PS)
1.0	Modification des ACL	11 mars 2013	Patrick Saladino (PS)

Diffusion

Unité	Nom	Mode de diffusion
DIT-SB	WinTeam, MO, KT	Electronique (courriel)
DIT-TI	RT	Electronique (courriel)
Utilisateurs des moyens informatiques de l'EPFL		Seulement la partie non technique, sur demande.

Description du service

Le service « Journalisation des requêtes DNS Windows » permet de disposer de journaux contenant toutes les requêtes DNS faites sur les serveurs DNS situés au sommet de la forêt Active Directory de l'EPFL (actuellement les trois contrôleurs de domaine AD1, AD2 et AD3), à des fins statistiques et de surveillance du réseau.

Le format des données stockées, leur durée de rétention ainsi que les droits d'accès à ces dernières seront explicitées dans les points qui suivent.

Horaire du service

La journalisation des requêtes DNS démarre en même temps que les autres services de la machine. Son horaire est donc celui de la machine hôte.

Disponibilité du service et fiabilité

Niveau de disponibilité	Nombre de pannes annuelles	Durée totale des indisponibilités annuelle
Excellent	1	1 heure
Très bon	2	2 heures
Bon	3	10 heures
Moyen	5	40 heures
Médiocre	Plus de 10	Plus de 40 heures

L'objectif est d'atteindre un niveau de disponibilité de service qualifié de très bon, soit une durée annuelle des indisponibilités non planifiées limitée à deux heures et ceci sur deux coupures maximum. Ces interruptions seront, la plupart du temps, dues à une mise à niveau des logiciels permettant la capture des requêtes DNS.

Support

Vu l'aspect assez pointu de la prestation et la criticité des machines qui l'hébergent, le support se fera directement auprès du gestionnaire du service, Patrick Saladino ou de son suppléant.

Téléphone : 179+32223 depuis n'importe quel poste téléphonique de l'EPFL
Téléphone : +41 79 535 99 42 depuis n'importe quel poste
Email : secure-it@epfl.ch

Nature des données stockées

Sans entrer dans des détails techniques qui seront explicités dans la seconde partie du document, les seules données stockées dans ces journaux sont les requêtes DNS faites depuis les postes du réseau EPNET vers les trois contrôleurs de domaine/serveurs DNS situés au sommet de la forêt intranet.epfl.ch. Ces données sont formées de/d' :

- Une empreinte temporelle (*timestamp* en anglais),
- L'adresse IP du client ainsi que le port TCP source,
- L'adresse IP du contrôleur de domaine recevant la requête ainsi que le port de destination
- Le type de requête,
- La requête proprement dite,
- Des détails purement techniques comme la classe, le numéro de séquence ainsi que la longueur des paramètres.

En voici trois exemples :

```
08:59:58.712416 IP 128.178.192.25.56168 > 128.178.15.229.53:  63224+ MX? epfl.ch. (25)
09:00:17.118360 IP 128.178.201.127.2804 > 128.178.15.229.53:  2+ PTR? 151.201.178.128.in-addr.arpa. (46)
09:00:19.624447 IP 128.178.81.6.65283   > 128.178.15.229.53:  63633+ A? 0-jv-w.channel.facebook.com. (45)
```

Confidentialité

Dans l'état actuel des choses, il ne nous est pas possible de faire facilement le lien direct entre une adresse IP (une machine à un instant donné) et son utilisateur. Ces données sont donc *anonymisées* par la force des choses.

Afin de protéger au mieux la vie privée de nos utilisateurs, elles ne seront accessibles que par les trois personnes responsables de la sécurité informatique des machines et du réseau, à savoir :

- Martin Ouwehand, DIT-SB
- Patrick Saladino, DIT-SB
- Nicolas Repond, DIT-SB / DIT-TI

Elles ne seront jamais communiquées brutes à des tiers sauf dans le cadre d'une enquête pénale, suite à une demande expresse d'un juge. Nous nous réservons toutefois le droit de partager les résultats de calculs statistiques effectués sur ces données brutes, en garantissant qu'ils soient parfaitement anonymes.

Durée de rétention

La durée de rétention de ces données a été fixée à quatre jours maximum (une tâche de nettoyage quotidienne purge toutes les entrées plus vieilles que trois jours). Les statistiques issues de ces journaux ne sont pas concernées par cette purge et pourraient potentiellement avoir une durée de vie illimitée.

Validité de cet OLA

Conditions valables depuis le 1er janvier 2014 pour l'année en cours.

FIN DE LA PARTIE GENERALE