

Distribution EOLE - Tâche #24483

Scénario # 24481 (Terminé (Sprint)): Tester la solution Racdata

Analyser les requêtes adressées au service Bind9 sur hestia.eole.lan

17/07/2018 16:37 - Daniel Dehennin

Statut:	Fermé	Début:	17/07/2018
Priorité:	Normal	Echéance:	
Assigné à:	Daniel Dehennin	% réalisé:	100%
Version cible:	sprint 2018 29-34 Equipe MENSUR (été 2018)	Temps estimé:	12.00 heures
		Temps passé:	4.50 heures
Description <p>Les logs de requêtes bind9 sur hestia.eole.lan arrivent en double dans le message syslog, par exemple :</p> <pre><30>2018-07-17T11:56:16+02:00 hestia named[13430]: 17-Jul-2018 11:56:16.268 queries: info: client 192.168.10.136#54998: query: castor.eole.lan IN AAAA + 17-Jul-2018 11:56:16.268 queries: info: client 192.168.10.136#54998: query: castor.eole.lan IN AAAA +</pre> <p>Le format est différent de celui fourni par défaut, il nous faut donc une configuration particulière.</p>			

Historique

#1 - 17/07/2018 16:37 - Daniel Dehennin

- Statut changé de Nouveau à En cours
- Assigné à mis à Daniel Dehennin

#2 - 17/07/2018 16:38 - Daniel Dehennin

Analyse des logs de requête bind9

Ajout de la configuration suivante sur racdata-test.eole.lan:

- Définition des **patterns** spécifiques à **bind9**

```
[root@racdata-test ~]# cat > /etc/logstash/patterns/bind9 <<EOF
BIND9_QUERY_FLAG_RECURSE [+~]
BIND9_QUERY_FLAG_SIGNED S
BIND9_QUERY_FLAG_EDNS E
BIND9_QUERY %{BIND9_TIMESTAMP:[query][timestamp]} queries: %{LOGLEVEL:loglevel}: client %{IP:[query][client][ip]}#%{POSINT:[query][client][port]:int}: query: %{GREEDYDATA:[query][request]} IN %{GREEDYDATA:[query][type]} %{BIND9_QUERY_FLAG_RECURSE:[query][flag][recurse]}%{BIND9_QUERY_FLAG_SIGNED:[query][flag][signed]}?%{BIND9_QUERY_FLAG_EDNS:[query][flag][edns]}? %{GREEDYDATA:message}
EOF
```

- Ajout de l'analyse des logs de **bind9**

```
[root@racdata-test ~]# cat > /etc/logstash/instances/analyse/filter-10-analyse-bind9.conf <<EOF
filter {
  if [program] == "named" {
    if [canal] {
      # Use canal test for heavy logs
      mutate {
        replace => { "canal" => "net" }
      }
    }
    grok {
      # Overwrite the "message" to get it unduplicated
      match => { "message" => "%{BIND9_QUERY}" }
    }
  }
}
```

```

        patterns_dir => [ "/etc/logstash/patterns" ]
        overwrite => [ "message" ]
        tag_on_failure => [ "named_parsing_failed" ]
        remove_tag => [ "_grokparsefailure" ]
        add_tag => ["DNS"]
    }
    if [syslog][ip] {
        mutate {
            copy => { "[syslog][ip]" => "source_host" }
        }
    }
    # Make the flags more readable
    if [query][flag][recurse] {
        translate {
            field => "[query][flag][recurse]"
            destination => "[query][recurse]"
            dictionary => {
                "+" => "yes"
                "-" => "no"
            }
            fallback => "unknown"
            override => true
            remove_field => "[query][flag][recurse]"
        }
    }
    if [query][flag][edns] == "E" {
        mutate {
            add_field => { "[query][edns]" => "yes" }
            remove_field => [ "[query][flag][edns]" ]
        }
    }
    elseif ! [query][flag][edns] {
        mutate {
            add_field => {
                "[query][edns]" => "no"
            }
        }
    }
    if [query][flag][signed] == "S" {
        mutate {
            add_field => { "[query][signed]" => "yes" }
            remove_field => [ "[query][flag][signed]" ]
        }
    }
    elseif ! [query][flag][signed] {
        mutate {
            add_field => {
                "[query][signed]" => "no"
            }
        }
    }
}
}
EOF

```

- Redémarrage du daemon d'analyse

```
[root@racdata-test ~]# systemctl restart logstash-analyse.service
```

- Vérification du démarrage

```

[root@racdata-test ~]# tail -n 0 -f /var/log/logstash/analyse/logstash.log
[2018-07-17T16:20:49,666][INFO ][logstash.outputs.rabbitmq] Connected to RabbitMQ at
[2018-07-17T16:20:50,858][INFO ][logstash.pipeline] Starting pipeline {"id"=>"main", "pipeline.workers"=>2, "pipeline.batch.size"=>125, "pipeline.batch.delay"=>5, "pipeline.max_inflight"=>250}
[2018-07-17T16:20:50,861][INFO ][logstash.pipeline] Pipeline main started
[2018-07-17T16:20:50,884][INFO ][logstash.agent] Successfully started Logstash API endpoint {:port=>9602}
[2018-07-17T16:20:50,885][INFO ][logstash.inputs.rabbitmq] Connected to RabbitMQ at

```

Résultats d'analyse

Après quelques instants, les premiers log de requêtes **bind9** sont analysées.

Vous devriez les voir dans l'interface **kibana** sous l'onglet **Discover**, voici ce que j'obtiens, au format JSON :

```
{
  [...]
  "process": {
    "name": "named",
    "id": 14414
  },
  [...]
  "query": {
    "request": "bp-eole.ac-dijon.fr",
    "flag": {},
    "recurse": "yes",
    "client": {
      "port": 33221,
      "ip": "192.168.10.142"
    },
    "signed": "no",
    "edns": "no",
    "type": "A",
    "timestamp": "17-Jul-2018 16:26:34.145"
  },
  [...]
  "syslog": {
    "severity": {
      "code": 6,
      "label": "informational"
    },
    "hostname": "hestia",
    "fqdn": "hestia.eole.lan",
    "pri": 30,
    "ip": "192.168.232.2",
    "raw": "<30>2018-07-17T16:26:34+02:00 hestia named[14414]: 17-Jul-2018 16:26:34.145 queries: info: client 192.168.10.142#33221: query: bp-eole.ac-dijon.fr IN A + 17-Jul-2018 16:26:34.145 queries: info: client 192.168.10.142#33221: query: bp-eole.ac-dijon.fr IN A +",
    "facility": {
      "code": 3,
      "label": "daemon"
    },
    "timestamp": "2018-07-17T16:26:34+02:00"
  },
  [...]
  "message": "17-Jul-2018 16:26:34.145 queries: info: client 192.168.10.142#33221: query: bp-eole.ac-dijon.fr IN A +",
  [...]
  "tags": [
    "DNS"
  ],
  [...]
}
<pre>
```

#3 - 17/07/2018 16:38 - Daniel Dehennin

- % réalisé changé de 0 à 100
- Restant à faire (heures) changé de 12.0 à 0.0

#4 - 18/07/2018 10:59 - Daniel Dehennin

- Description mis à jour

#5 - 18/07/2018 16:33 - Daniel Dehennin

J'ai modifié la configuration pour faire une résolution inverse sur l'IP des clients

```
@@ -57,5 +55,23 @@
    }
  }
}
+   if [query][client][ip] {
+     dnstimeout {
+       reverse => {
+         "[query][client][ip]" => "[query][client][host]"
+       }
+       action => "replace"
+       failed_cache_size => 10000
+       failed_cache_ttl => 86400
+       hit_cache_size => 10000
+       hit_cache_ttl => 86400
+       timeout => 0.1
+     }
+   }
+   if ! [query][client][host] {
+     mutate {
+       copy => { "[query][client][ip]" => "[query][client][host]" }
+     }
+   }
+ }
```

#6 - 19/07/2018 09:38 - Scrum Master

- Statut changé de En cours à Résolu
- Tâche parente changé de #24481 à #24475

#7 - 19/07/2018 09:38 - Scrum Master

- *Tâche parente changé de #24475 à #24481*

#8 - 27/08/2018 09:55 - Daniel Dehennin

- *Statut changé de Résolu à Fermé*