**Compte rendu :**

# I.1. Installation, test et configuration de Logstash

## I.1) Installation logstash

Après avoir installer logstash on vérifie sa version pour voir que tout marche bien :

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

## I.1.2. Test de Logstash

logstash --path.data /tmp/logstash\_data --log.level=error -e "input { stdin {} } output { stdout { codec => rubydebug } }"

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

## I.1.3. Configuration de Logstash

Personnaliser le lancement de logstash avec la configuration :



Puis saisie d’un log : Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

# I.2. Fonctionnement de Logstash

## I.2.1. Arborescence des fichiers

Une image contenant texte, capture d’écran, menu, Police

Le contenu généré par l’IA peut être incorrect.

## I.2.2. Pipelines Logstash

C’est le fichier de conf lancé par notre pipeline :

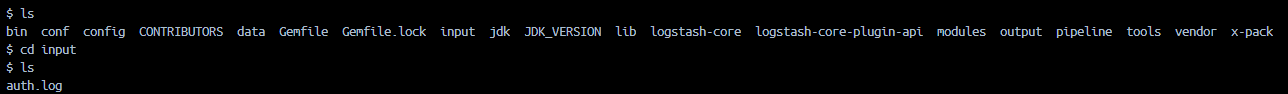
Une image contenant texte, capture d’écran, Police, conception

Le contenu généré par l’IA peut être incorrect.

**II. Exercices**

**II.1. Exercice guidé**

Création du fichier auth.log avec son contenu sous input :



Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Création du dossier auth sous conf, ainsi que du fichier de configuration logstash.conf :

Une image contenant capture d’écran, texte

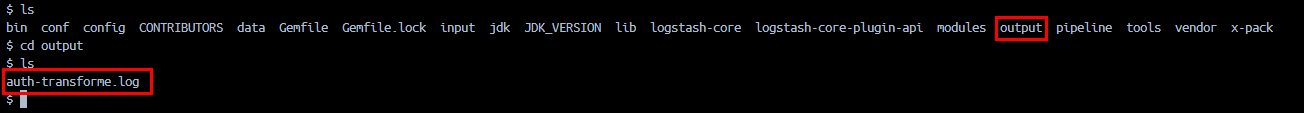
Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

Ici on n’oublie pas de préciser le chemin de notre fichier input et output.

Création du fichier output :



Puis on lance la commande : 

On regarde le résultat dans notre fichier output :

Une image contenant texte, capture d’écran, affichage, logiciel

Le contenu généré par l’IA peut être incorrect.

Comme expliqué dans le TP, on peut voir que « date » et « pid » ne possèdent pas de guillemets car leurs valeurs ont bien été convertis, en date et en nombre.

**II.2. Logs multilines**

Dans un premier temps on change le contenu du fichier auth.log :

Une image contenant texte, Police, logiciel, capture d’écran

Le contenu généré par l’IA peut être incorrect.

On peut maintenant voir que on a des logs multilines.

Si on relance la configuration précédente avec ses nouveaux logs ont obtient une erreur `\_grokparsefailure`pour la ligne 1 et 5.

Pour résoudre ce problème il nous faut modifier le fichier logstash.conf présente sous conf/auth : Une image contenant texte, capture d’écran, logiciel, affichage

Le contenu généré par l’IA peut être incorrect.

En précisant le codec multilines on indique à logstash que notre intput va être au format multilines.

Cela nous empêche d’avoir l’erreur `\_grokparsefailure` et prend bien en compte tout le log même s’il est sur deux lignes.

Maintenant on peut donc lancer la commande : 

Le résultat dans notre fichier output est affiché dans les erreurs `\_grokparsefailure`, et on peut voir qu’il est précisé pour le log 1 et 5 qu’ils étaient multilines :

Une image contenant texte, capture d’écran, affichage, logiciel

Le contenu généré par l’IA peut être incorrect.

**II.3. Apache access logs**

Dans cette exercice nos logs en input ont une structure différente. Il s’agit de logs au format Apache Combined Log Format, qui enregistre les requêtes HTTP traitées par le serveur web.

Pour trouver la structure on prend ce log (le premier):

83.149.9.216 - - [17/May/2015:10:05:03 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"

On va prendre les champs 1 par 1 :

* **83.149.9.216** : correspond à l’adresse IP du client qui a effectué la requête
* **‘-‘** : identité RFC du client, écrit ‘-‘ car non utilisé
* **‘-‘** : correspond au nom d’utilisateur si une authentification était requise sinon on laisse ‘-‘.
* **[17/May/2015:10:05:03 +0000]** : correspond au timestamp au format : [jour/Mois/année:HH:mm:ss Z] avec Z qui correspond au fuseau horaire.
* **"GET** : qui correspond à la méthode http demandée
* **/presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1** : qui correspond à la ressource demandée par la requête http
* **200** : correspond au code de réponse de la requête
* **203023** : correspond à la taille de la réponse retournée par la requête http
* [**http://semicomplete.com/presentations/logstash-monitorama-2013/**](http://semicomplete.com/presentations/logstash-monitorama-2013/) : correspond à l’url de la page d’où vient le visiteur
* **"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"** : information concernant le navigateur et système d’exploitation du client.

Ici on peut donc décomposer notre grok comme suit :

* %{IPORHOST:clientip} → IP ou Host du client
* %{HTTPDUSER:ident} → Identifiant utilisateur HTTP (souvent -)
* %{HTTPDUSER:auth} → Utilisateur authentifié (ou - si pas d'authentification)
* \[%{HTTPDATE:timestamp}\] → Date et heure de la requête (entourée de [])
* "%{WORD:verb} %{NOTSPACE:request} HTTP/%{NUMBER:httpversion}" → Méthode HTTP + URL demandée + version HTTP
* %{NUMBER:response:int} → Code de réponse HTTP (200, 404, etc.)
* (?:-|%{NUMBER:bytes:int}) → Nombre d’octets retournés
* (?:-|%{NUMBER:bytes:int}) → Gère les cas où la taille est - (inconnue)
* %{QS:referrer} → Référent (d’où vient la requête)
* %{QS:agent} → pour les infos sur le navigateur et le système d’exploitation du client

Il faut également formater la date et les champs sous format nombre.

Cela nous donne donc le fichier de conf :

Une image contenant texte, capture d’écran, affichage, logiciel

Le contenu généré par l’IA peut être incorrect.

Cela nous retourne donc le résultat en output suivant :

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:03 +0000] \"GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1\" 200 203023 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/kibana-search.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.559412817*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *203023,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:43 +0000] \"GET /presentations/logstash-monitorama-2013/images/kibana-dashboard3.png HTTP/1.1\" 200 171717 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/kibana-dashboard3.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.561459617*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *171717,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:47 +0000] \"GET /presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1\" 200 26185 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/plugin/highlight/highlight.js"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.562025336*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *26185,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:12 +0000] \"GET /presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js HTTP/1.1\" 200 7697 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.562584571*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *7697,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:07 +0000] \"GET /presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1\" 200 2892 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/plugin/notes/notes.js"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.562983165*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *2892,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:34 +0000] \"GET /presentations/logstash-monitorama-2013/images/sad-medic.png HTTP/1.1\" 200 430406 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/sad-medic.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.563342036*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *430406,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:57 +0000] \"GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Bold.ttf HTTP/1.1\" 200 38720 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/css/fonts/Roboto-Bold.ttf"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.563683825*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *38720,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:50 +0000] \"GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf HTTP/1.1\" 200 41820 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.564077112*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *41820,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:24 +0000] \"GET /presentations/logstash-monitorama-2013/images/frontend-response-codes.png HTTP/1.1\" 200 52878 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/frontend-response-codes.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.564682508*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *52878,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:50 +0000] \"GET /presentations/logstash-monitorama-2013/images/kibana-dashboard.png HTTP/1.1\" 200 321631 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/kibana-dashboard.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.565277229*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *321631,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:46 +0000] \"GET /presentations/logstash-monitorama-2013/images/Dreamhost\_logo.svg HTTP/1.1\" 200 2126 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/Dreamhost\_logo.svg"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.565822896*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *2126,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:11 +0000] \"GET /presentations/logstash-monitorama-2013/images/kibana-dashboard2.png HTTP/1.1\" 200 394967 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/kibana-dashboard2.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.566185773*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *394967,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:19 +0000] \"GET /presentations/logstash-monitorama-2013/images/apache-icon.gif HTTP/1.1\" 200 8095 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/apache-icon.gif"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.566543333*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *8095,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:33 +0000] \"GET /presentations/logstash-monitorama-2013/images/nagios-sms5.png HTTP/1.1\" 200 78075 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/nagios-sms5.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.566876861*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *78075,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:00 +0000] \"GET /presentations/logstash-monitorama-2013/images/redis.png HTTP/1.1\" 200 25230 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/redis.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.567206184*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *25230,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:25 +0000] \"GET /presentations/logstash-monitorama-2013/images/elasticsearch.png HTTP/1.1\" 200 8026 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/elasticsearch.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.567522069*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *8026,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:59 +0000] \"GET /presentations/logstash-monitorama-2013/images/logstashbook.png HTTP/1.1\" 200 54662 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/logstashbook.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.567843441*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *54662,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:30 +0000] \"GET /presentations/logstash-monitorama-2013/images/github-contributions.png HTTP/1.1\" 200 34245 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/github-contributions.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.568155311*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *34245,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:53 +0000] \"GET /presentations/logstash-monitorama-2013/css/print/paper.css HTTP/1.1\" 200 4254 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/css/print/paper.css"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.568499343*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *4254,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:24 +0000] \"GET /presentations/logstash-monitorama-2013/images/1983\_delorean\_dmc-12-pic-38289.jpeg HTTP/1.1\" 200 220562 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/1983\_delorean\_dmc-12-pic-38289.jpeg"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.569321042*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *220562,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:54 +0000] \"GET /presentations/logstash-monitorama-2013/images/simple-inputs-filters-outputs.jpg HTTP/1.1\" 200 1168622 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/simple-inputs-filters-outputs.jpg"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.569637088*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *1168622,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:33 +0000] \"GET /presentations/logstash-monitorama-2013/images/tiered-outputs-to-inputs.jpg HTTP/1.1\" 200 1079983 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/presentations/logstash-monitorama-2013/images/tiered-outputs-to-inputs.jpg"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.569948387*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *1079983,*

       "referrer" *=>* "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "83.149.9.216"*,*

        "message" *=>* "83.149.9.216 - - [17/May/2015:10:05:56 +0000] \"GET /favicon.ico HTTP/1.1\" 200 3638 \"-\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"\r"*,*

        "request" *=>* "/favicon.ico"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.571906550*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *3638,*

       "referrer" *=>* "\"-\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "24.236.252.67"*,*

        "message" *=>* "24.236.252.67 - - [17/May/2015:10:05:40 +0000] \"GET /favicon.ico HTTP/1.1\" 200 3638 \"-\" \"Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:26.0) Gecko/20100101 Firefox/26.0\"\r"*,*

        "request" *=>* "/favicon.ico"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.572333571*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:26.0) Gecko/20100101 Firefox/26.0\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *3638,*

       "referrer" *=>* "\"-\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "93.114.45.13"*,*

        "message" *=>* "93.114.45.13 - - [17/May/2015:10:05:14 +0000] \"GET /articles/dynamic-dns-with-dhcp/ HTTP/1.1\" 200 18848 \"http://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCwQFjAB&url=http%3A%2F%2Fwww.semicomplete.com%2Farticles%2Fdynamic-dns-with-dhcp%2F&ei=W88AU4n9HOq60QXbv4GwBg&usg=AFQjCNEF1X4Rs52UYQyLiySTQxa97ozM4g&bvm=bv.61535280,d.d2k\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"\r"*,*

        "request" *=>* "/articles/dynamic-dns-with-dhcp/"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.572694645*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *18848,*

       "referrer" *=>* "\"http://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCwQFjAB&url=http%3A%2F%2Fwww.semicomplete.com%2Farticles%2Fdynamic-dns-with-dhcp%2F&ei=W88AU4n9HOq60QXbv4GwBg&usg=AFQjCNEF1X4Rs52UYQyLiySTQxa97ozM4g&bvm=bv.61535280,d.d2k\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "93.114.45.13"*,*

        "message" *=>* "93.114.45.13 - - [17/May/2015:10:05:04 +0000] \"GET /reset.css HTTP/1.1\" 200 1015 \"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"\r"*,*

        "request" *=>* "/reset.css"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.573210082*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *1015,*

       "referrer" *=>* "\"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "93.114.45.13"*,*

        "message" *=>* "93.114.45.13 - - [17/May/2015:10:05:45 +0000] \"GET /style2.css HTTP/1.1\" 200 4877 \"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"\r"*,*

        "request" *=>* "/style2.css"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.575504012*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *4877,*

       "referrer" *=>* "\"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "93.114.45.13"*,*

        "message" *=>* "93.114.45.13 - - [17/May/2015:10:05:14 +0000] \"GET /favicon.ico HTTP/1.1\" 200 3638 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"\r"*,*

        "request" *=>* "/favicon.ico"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.576736732*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *3638,*

       "referrer" *=>* "\"-\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "93.114.45.13"*,*

        "message" *=>* "93.114.45.13 - - [17/May/2015:10:05:17 +0000] \"GET /images/jordan-80.png HTTP/1.1\" 200 6146 \"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"\r"*,*

        "request" *=>* "/images/jordan-80.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*19.579591959*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *6146,*

       "referrer" *=>* "\"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

{

       "response" *=>* *200,*

       "clientip" *=>* "93.114.45.13"*,*

        "message" *=>* "93.114.45.13 - - [17/May/2015:10:05:21 +0000] \"GET /images/web/2009/banner.png HTTP/1.1\" 200 52315 \"http://www.semicomplete.com/style2.css\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"\r"*,*

        "request" *=>* "/images/web/2009/banner.png"*,*

           "auth" *=>* "-"*,*

          "ident" *=>* "-"*,*

           "host" *=>* "401ca1a41a18"*,*

     "@timestamp" *=>* *2025-03-15T00*:07*:*40.617168412*Z*,

    "httpversion" *=>* *1.1,*

          "agent" *=>* "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\""*,*

           "verb" *=>* "GET"*,*

          "bytes" *=>* *52315,*

       "referrer" *=>* "\"http://www.semicomplete.com/style2.css\""*,*

           "path" *=>* "/usr/share/logstash/input/auth.log"*,*

       "@version" *=>* "1"

}

**II.4. Data venant d’un CSV**

Dans notre fichier input on ajoute les logs csv :

Une image contenant texte, capture d’écran, Police, logiciel

Le contenu généré par l’IA peut être incorrect.

Puis on modifie notre fichier de conf pour formatter des données de types csv :

Une image contenant texte, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

Dans notre fichier de conf on créer le filter :

* On précise que c’est des logs csv
* On précise le séparateur entre nos données csv, ici c’est la virgule
* On ignore les colonnes vides pour ne pas avoir des champs vide dans la sortie output
* Et on ajoute l’auto détecte de colonne.

Cela nous permet de préciser le filtre à appliquer sur nos logs csv.

Concernant le formatage on décide de formatter le code postal en integer et d’enlever les espaces autour des initiales des villes, dans le cas ou c’est marqué ‘ NJ’ comme dans nos logs par exemple.

Tous ces paramètres permettent de bien formatter notre sortie output.

Maintenant on peut donc lancer la commande : 

Voici notre output :

Une image contenant texte, capture d’écran, affichage

Le contenu généré par l’IA peut être incorrect.

**II.5. JSON logs**

Dans notre fichier input on ajouter les logs web au format json :

Une image contenant texte, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Puis on modifie notre fichier de conf pour formatter des données de types json :

Une image contenant texte, affichage, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

Dans le fichier de conf on ajoute :

json { source => "message" }  
  
cela permet de prendre le contenu du champ message et de l’interpréter comme un objet JSON.

Ensuite dans date on récupère la valeur du champ timestamp (fourni par le JSON) et la convertit en un objet date, que Logstash stockera dans @timestamp (le champ standard de Logstash pour la date/heure d’événement).

Avec match => ["timestamp", "ISO8601"] indique à Logstash d’utiliser le format ISO8601 pour la conversion.

Puis avec mutate on transforme certain champs json dans un meilleur type (valeur numérique).

Pour finir on supprime le champ timestamp d’origine, car comme on l’a déjà converti en @timestamp, le champ brut timestamp n’est plus nécessaire.

Tous ces paramètres permettent de bien formatter notre sortie output.

Maintenant on peut donc lancer la commande :  pour obtenir l’output suivant :

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:03.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:03 +0000] \"GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1\" 200 203023 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/kibana-search.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 203023,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:43.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:43 +0000] \"GET /presentations/logstash-monitorama-2013/images/kibana-dashboard3.png HTTP/1.1\" 200 171717 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/kibana-dashboard3.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 171717,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:47.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:47 +0000] \"GET /presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1\" 200 26185 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/plugin/highlight/highlight.js",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 26185,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:12.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:12 +0000] \"GET /presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js HTTP/1.1\" 200 7697 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 7697,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:07.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:07 +0000] \"GET /presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1\" 200 2892 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/plugin/notes/notes.js",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 2892,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:34.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:34 +0000] \"GET /presentations/logstash-monitorama-2013/images/sad-medic.png HTTP/1.1\" 200 430406 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/sad-medic.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 430406,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:57.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:57 +0000] \"GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Bold.ttf HTTP/1.1\" 200 38720 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/css/fonts/Roboto-Bold.ttf",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 38720,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:50.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:50 +0000] \"GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf HTTP/1.1\" 200 41820 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 41820,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:24.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:24 +0000] \"GET /presentations/logstash-monitorama-2013/images/frontend-response-codes.png HTTP/1.1\" 200 52878 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/frontend-response-codes.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 52878,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:50.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:50 +0000] \"GET /presentations/logstash-monitorama-2013/images/kibana-dashboard.png HTTP/1.1\" 200 321631 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/kibana-dashboard.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 321631,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:46.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:46 +0000] \"GET /presentations/logstash-monitorama-2013/images/Dreamhost\_logo.svg HTTP/1.1\" 200 2126 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/Dreamhost\_logo.svg",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 2126,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:11.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:11 +0000] \"GET /presentations/logstash-monitorama-2013/images/kibana-dashboard2.png HTTP/1.1\" 200 394967 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/kibana-dashboard2.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 394967,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:19.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:19 +0000] \"GET /presentations/logstash-monitorama-2013/images/apache-icon.gif HTTP/1.1\" 200 8095 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/apache-icon.gif",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 8095,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:33.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:33 +0000] \"GET /presentations/logstash-monitorama-2013/images/nagios-sms5.png HTTP/1.1\" 200 78075 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/nagios-sms5.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 78075,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:00.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:00 +0000] \"GET /presentations/logstash-monitorama-2013/images/redis.png HTTP/1.1\" 200 25230 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/redis.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 25230,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:25.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:25 +0000] \"GET /presentations/logstash-monitorama-2013/images/elasticsearch.png HTTP/1.1\" 200 8026 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/elasticsearch.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 8026,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:59.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:59 +0000] \"GET /presentations/logstash-monitorama-2013/images/logstashbook.png HTTP/1.1\" 200 54662 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/logstashbook.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 54662,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:30.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:30 +0000] \"GET /presentations/logstash-monitorama-2013/images/github-contributions.png HTTP/1.1\" 200 34245 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/github-contributions.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 34245,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:53.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:53 +0000] \"GET /presentations/logstash-monitorama-2013/css/print/paper.css HTTP/1.1\" 200 4254 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/css/print/paper.css",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 4254,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:24.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:24 +0000] \"GET /presentations/logstash-monitorama-2013/images/1983\_delorean\_dmc-12-pic-38289.jpeg HTTP/1.1\" 200 220562 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/1983\_delorean\_dmc-12-pic-38289.jpeg",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 220562,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:54.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:54 +0000] \"GET /presentations/logstash-monitorama-2013/images/simple-inputs-filters-outputs.jpg HTTP/1.1\" 200 1168622 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/simple-inputs-filters-outputs.jpg",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 1168622,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:33.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:33 +0000] \"GET /presentations/logstash-monitorama-2013/images/tiered-outputs-to-inputs.jpg HTTP/1.1\" 200 1079983 \"http://semicomplete.com/presentations/logstash-monitorama-2013/\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"http://semicomplete.com/presentations/logstash-monitorama-2013/\"",

"clientip" => "83.149.9.216",

"request" => "/presentations/logstash-monitorama-2013/images/tiered-outputs-to-inputs.jpg",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 1079983,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:56.000Z,

"message" => "83.149.9.216 - - [17/May/2015:10:05:56 +0000] \"GET /favicon.ico HTTP/1.1\" 200 3638 \"-\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"referrer" => "\"-\"",

"clientip" => "83.149.9.216",

"request" => "/favicon.ico",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 3638,

"agent" => "\"Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:40.000Z,

"message" => "24.236.252.67 - - [17/May/2015:10:05:40 +0000] \"GET /favicon.ico HTTP/1.1\" 200 3638 \"-\" \"Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:26.0) Gecko/20100101 Firefox/26.0\"",

"referrer" => "\"-\"",

"clientip" => "24.236.252.67",

"request" => "/favicon.ico",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 3638,

"agent" => "\"Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:26.0) Gecko/20100101 Firefox/26.0\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:14.000Z,

"message" => "93.114.45.13 - - [17/May/2015:10:05:14 +0000] \"GET /articles/dynamic-dns-with-dhcp/ HTTP/1.1\" 200 18848 \"http://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCwQFjAB&url=http%3A%2F%2Fwww.semicomplete.com%2Farticles%2Fdynamic-dns-with-dhcp%2F&ei=W88AU4n9HOq60QXbv4GwBg&usg=AFQjCNEF1X4Rs52UYQyLiySTQxa97ozM4g&bvm=bv.61535280,d.d2k\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"referrer" => "\"http://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCwQFjAB&url=http%3A%2F%2Fwww.semicomplete.com%2Farticles%2Fdynamic-dns-with-dhcp%2F&ei=W88AU4n9HOq60QXbv4GwBg&usg=AFQjCNEF1X4Rs52UYQyLiySTQxa97ozM4g&bvm=bv.61535280,d.d2k\"",

"clientip" => "93.114.45.13",

"request" => "/articles/dynamic-dns-with-dhcp/",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 18848,

"agent" => "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:04.000Z,

"message" => "93.114.45.13 - - [17/May/2015:10:05:04 +0000] \"GET /reset.css HTTP/1.1\" 200 1015 \"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"referrer" => "\"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\"",

"clientip" => "93.114.45.13",

"request" => "/reset.css",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 1015,

"agent" => "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:45.000Z,

"message" => "93.114.45.13 - - [17/May/2015:10:05:45 +0000] \"GET /style2.css HTTP/1.1\" 200 4877 \"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"referrer" => "\"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\"",

"clientip" => "93.114.45.13",

"request" => "/style2.css",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 4877,

"agent" => "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:14.000Z,

"message" => "93.114.45.13 - - [17/May/2015:10:05:14 +0000] \"GET /favicon.ico HTTP/1.1\" 200 3638 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"referrer" => "\"-\"",

"clientip" => "93.114.45.13",

"request" => "/favicon.ico",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 3638,

"agent" => "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:17.000Z,

"message" => "93.114.45.13 - - [17/May/2015:10:05:17 +0000] \"GET /images/jordan-80.png HTTP/1.1\" 200 6146 \"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"referrer" => "\"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/\"",

"clientip" => "93.114.45.13",

"request" => "/images/jordan-80.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 6146,

"agent" => "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

{

"verb" => "GET",

"@timestamp" => 2015-05-17T10:05:21.000Z,

"message" => "93.114.45.13 - - [17/May/2015:10:05:21 +0000] \"GET /images/web/2009/banner.png HTTP/1.1\" 200 52315 \"http://www.semicomplete.com/style2.css\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"referrer" => "\"http://www.semicomplete.com/style2.css\"",

"clientip" => "93.114.45.13",

"request" => "/images/web/2009/banner.png",

"@version" => "1",

"host" => "localhost",

"auth" => "-",

"ident" => "-",

"bytes" => 52315,

"agent" => "\"Mozilla/5.0 (X11; Linux x86\_64; rv:25.0) Gecko/20100101 Firefox/25.0\"",

"httpversion" => 1.1,

"path" => "/usr/share/logstash/input/auth.log",

"response" => 200

}

**III. Questions ouvertes**

### 1) Est-ce que la transformation des données est simple ?

La transformation des données avec Logstash peut être simple ou complexe selon plusieurs facteurs :

* La structure et la régularité des données sources.
* La nécessité d’utiliser plusieurs filtres (ex : grok, mutate, date).
* Le niveau de connaissance des expressions régulières et des formats de logs.
* La gestion des erreurs et l’interprétation des messages d’échec (\_grokparsefailure).

Pour des logs bien formatés et homogènes, la transformation est relativement simple. En revanche, lorsqu’il faut gérer des logs multilignes ou des structures de données complexes, cela peut vite devenir compliqué.

### 2) Les données de l'exercice II.3 et II.5 sont les mêmes : lesquelles sont plus simples à traiter ? Et pourquoi ?

Les logs JSON de l’exercice II.5 sont plus simples à traiter que les logs Apache de II.3 parce que Les logs JSON ont déjà une structure clé-valeur explicite, ce qui facilite leur extraction avec le filtre json de Logstash contrairement aux logs Apache qui nécessitent un parsing basé sur un grok pattern, ce qui peut être plus complexe à écrire et ajuster.

Les formats de logs traditionnels comme Apache demandent plus de travail pour extraire chaque champ (adresse IP, timestamp, requête, statut, etc.), tandis que le JSON est plus directement exploitable.

### 3) Dans le cadre d'exploitation de logs, vaut-il mieux formater ses logs dans une application elle-même ou à postériori, dans une phase de transformation ?

Cela dépend des contraintes et de l’environnement :

* Formatage dans l’application (à la source) :
* Avantage : Moins de traitement en aval, moins de risque d’erreurs de parsing.
* Inconvénient : Moins de flexibilité si le format doit changer, dépend fortement du code de l’application.
* Transformation avec Logstash (post-traitement) :
  1. Avantage : Plus de flexibilité, possibilité de modifier facilement le format sans toucher au code des applications.
  2. Inconvénient : Plus de charge sur le pipeline de traitement, potentiellement plus lent si les volumes de logs sont très élevés.

En général, il est préférable de standardiser le format des logs à la source (ex: JSON) pour faciliter l’ingestion et la transformation, tout en gardant une phase de traitement pour les enrichissements ou corrections nécessaires.