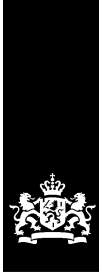

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Voorbeeldinstallatie BRPLogging

Versie 1.0

Datum Augustus 2015
Status Release

Documentinformatie

Titel	Voorbeeldinstallatie BRP Logging
Datum	Augustus 2015
Versie	1.0
Status	Release
Documentlocatie	https://www.modernodam.nl/svn/brp-code/trunk/build/distributie/src/main/doc/

Versiehistorie

Versie	Datum	Omschrijving
1.0	Augustus 2015	Final versie voor oplevering

INHOUDSOPGAVE

1 Inleiding

1.1 Doel

Handleiding voor het installeren van centrale logging of een client die verbindt met de centrale logging voor de BRP services.

1.2 Achtergrond

Informatieoverdracht vanuit applicatie ontwikkeling naar operationeel beheer.

1.3 Scope

Dit document is bedoeld voor operationeel beheerders van de BRP Levering Servicesen beschrijft hoe de centrale logging kan worden ingericht.

1.4 Aannames

Kennis van Unix is vereist. Ook wordt aangenomen dat de volgende poorten openstaan op de servers die onderling een cluster vormen via ElasticSearch:
TCP: 9200 (http connectie), 9300-9305 (transport connectie)
UDP: 54328 (multicast)

1.5 Leeswijzer

Operationeel beheerders die de BRP logging installeren kunnen bij hoofdstuk 2 beginnen. Dit hoofdstuk gaat in op de installatie, setup en configuratie van hetlogging systeem. Dit logging systeem bestaat uit vier onderdelen:

- Logstash, een input processor die van diverse type inputs de logging op kan slaan in bijvoorbeeld ElasticSearch. (http://www.logstash.net)
- ElasticSearch, de databak waar alle logging in kan worden opgeslagen (geclusterd) (http://www.elasticsearch.org)
- Kibana, de applicatie waarin dashboards kunnen worden gemaakt om de logging in te kunnen zien. (http://www.elasticsearch.org/overview/kibana)
- Elastic HQ, de applicatie waarin het Elasticsearch cluster kan worden ingezien en indexen geoptimaliseerd en verwijderd.

2 ElasticSearch

Dit hoofdstuk beschrijft de installatie, configuratie en het opstarten van ElasticSearch op een Unix omgeving. Let op dat de eerder genoemde poorten open dienen te staan voor ElasticSearch:
TCP: 9200 (http connectie), 9300-9305 (transport connectie)
UDP: 54328 (multicast)

2.1.1 Installatie

Log in op de gewenste server en verkrijg root-rechten.

Plaats het volgende bestand in de `/tmp` directory:

```
artefacten/logging/elasticsearch-1.3.1.noarch.rpm
```

InstalleerElasticSearch:

```
rpm -i/tmp/elasticsearch-1.3.1.noarch.rpm
```

Zorg ervoor dat ElasticSearch opstart bij een reboot:

```
sudo /sbin/chkconfig --addelasticsearch
```

2.1.2 Configuratie

ElasticSearch dient geconfigureerd te worden, dit zorgt ervoor dat andere instanties aan kunnen sluiten op dezelfde cluster.
Hiervoor dient het algemene configuratiebestand van ElasticSearch te worden aangepast, te vinden op: */etc/elasticsearch/elasticsearch.yml*
Zorg dat de clusternaam voor alle Elasticsearch servers hetzelfde is en kies per deel van de infrastructuur een duidelijke naam voor `CLUSTERNAAM` (Bijvoorbeeld BRP-PROEFTUIN of BRP-ACCEPTATIE).
Hierbij kan de node_name (`NAAMVANDESERVER`) gewijzigd worden in een functioneel identificerende naam voor de server. (Bijvoorbeeld PROEFTUIN-LINKS-APP01 of PROEFTUIN-LINKS-MESSAGING)
Wijzig de *cluster.name* naar "`CLUSTERNAAM`"
Wijzig de *node.name* naar een identificerende naam voor de server zoals "`NAAMVANDESERVER`"

2.1.3 Starten

ElasticSearch kan nu gestart worden.
Gebruik hiervoor bijvoorbeeld het commando: */etc/init.d/elasticsearch start* of `service elasticsearch start`
Om te verifieren dat ElasticSearch correct is gestart kun je met je browser naar het volgende adres: http://servernaam:9200
Hier zul je dan data te zien krijgen van ElasticSearch.

3 Logstash

Dit hoofdstuk beschrijft de installatie, configuratie en het opstarten van Logstash op een Unix omgeving.

3.1.1 Installatie

Log in op de gewenste server en verkrijg root-rechten.

Plaats de volgende bestanden in de `/tmp` directory:

```
artefacten/logging/logstash-1.4.2-1_2c0f5a1.noarch.rpm
artefacten/logging/logstash-contrib-1.4.2-1_efd53ef.noarch.rpm
```

InstalleerLogstash:

```
rpm -i --nodeps/tmp/logstash-1.4.2-1_2c0f5a1.noarch.rpm
```

Installeer de contribplugins (onder andere nodig voor de jmx input plugin)

```
rpm –i --nodeps /tmp/logstash-contrib-1.4.2-1_efd53ef.noarch.rpm
```

Zorg ervoor dat Logstash opstart bij een reboot:

```
sudo /sbin/chkconfig --addlogstash
```

3.1.2 Configuratie

Logstash dient geconfigureerd te worden. Hierin wordt de input, eventuele filtering en de output vastgelegd. Maak hiervoor het volgende configuratiebestand aan:
`/etc/logstash/conf.d/logstash.conf`

De inhoud van dit bestand dient als volgt te zijn:

```
input {
  file {
    codec =>json { charset => "UTF-8"}
    type => "BRP-Log"
    path => "/opt/tomcat/logs/brp-mdc.log"
  }
}
filter {
}
output {
  elasticsearch {
    host => "HOSTNAAM"
    cluster => "CLUSTERNAAM"
    node_name => "NAAMVANDESERVER"
    protocol => "transport"
    index =>"omgeving-%{+YYYY.MM.dd}"
  }
}
```

Hierbij is de HOSTNAAM op de centrale logging server gewoon localhost, maar voor de applicatie servers waar logstash wordt geinstalleerd dient dit de hostnaam te zijn van de centrale logging server, dus bijvoorbeeld logging.modernodam.nl.
Let op dat de CLUSTERNAAM hetzelfde is als de clusternaam die je in het voorgaande hoofdstuk gegeven hebt aan het Elasticsearch cluster.

Belangrijk is hier dat de OMGEVING waarde dusdanig gekozen wordt dat alle logging van een bepaalde omgeving in dezelfde index komt. Standaard staat de index op logstash-%{+YYYY.MM.DD}, indien de logging server voor meerdere omgevingen

wordt gebruikt (zoals bijvoorbeeld twee proeftuin omgevingen), dan kan je hiermee ervoor zorgen dat de indexen gescheiden blijven. LET OP: de indexnaam moet in kleine letters geschreven worden. Dus geen hoofdletters!

Path verwijst naar de logging-file die de BRP vult met logmeldingen. Let op dat de logstash-user op de server wel toegang heeft tot de logging-file. Mogelijk dient de logstash-user aan de tomcat-group te worden toegevoegd of dient de toegang van de directories van tomcat te worden versoepeld ("`chmod 755`" geeft andere users zoals de logstash-user toegang tot de bestanden in die mappen).

3.1.3 Starten

Logstashkan nu gestart worden.
Gebruik hiervoor bijvoorbeeld het commando: */etc/init.d/*l*ogstashstart*
of `service logstash start`

4 Kibana

Dit hoofdstuk beschrijft de installatie van Kibana op een Unix omgeving.

4.1.1 Installatie

Log in op de gewenste server en verkrijg root-rechten.

Plaats het volgende bestand in de `/tmp` directory:

```
artefacten/logging/kibana-3.1.0.tar.gz
```

4.1.2 Configuratie

Pak het bestandsarchief uit en wijzig het bestand *config.js*en wijzig de parameter "`elasticsearch`" naar enkel de hostname van je ElasticSearch server.

4.1.3 Starten / beschikbaar stellen

Kibana kan beschikbaar gesteld worden, door de uitgepakte directory inclusief gewijzigde configuratie op je webserver te plaatsen.
Ga met je browser naar je webserver. Als er geen foutmelding getoond wordt in Kibana, heb je Kibana juist geconfigureerd.

5 Elastic HQ

Dit hoofdstuk beschrijft de installatie van Elastic HQ op een Unix omgeving.

5.1.1 Installatie

Plaats het volgende bestand in de `/tmp` directory:

```
artefacten/logging/royrusso-elasticsearch-HQ-603ae9e.zip
```

5.1.2 Starten / beschikbaar stellen

Elastic HQ kan beschikbaar gesteld worden, door de uitgepakte directory inclusief gewijzigde configuratie op je webserver te plaatsen.
Ga met je browser naar je webserver. Als er geen foutmelding getoond wordt in Elastic HQ, heb je Elastic HQ juist geconfigureerd.
Nu kun je connecten naar Elastic HQ door de url van de server waar Elasticsearch staat in te vullen aangevuld met poort 9200. Bijvoorbeeld: logging.modernodam.nl:9200.

6 Aandachtspunten onderhoud

6.1 Elasticsearch indexen

Elasticsearch maakt per dag een index aan. De logging kan naar loop van tijd worden opgeschoond, waarbij de periode per omgeving anders zal zijn. Op de ontwikkel omgeving is een termijn van 3 dagen genoeg, op de proeftuin zal dit eerder richting een maand gaan. Operationeel wellicht nog langer. Daarnaast is dit per index afhankelijk. De logging van applicaties is niet noodzakelijk om die lang te bewaren, logging die gaat over aantallen berichten is echter weer een ander verhaal. Daarom is het van belang om de juiste tag's mee te geven aan een logmessage. Voorlopig kan onderstaand script gebruikt worden om via een cronjob de overbodige indexen te verwijderen.

https://github.com/andreioprisan/logstash-elasticsearch-backup/blob/master/logstash-elasticsearch-cleanup.sh

6.2 Logrotatie

Voor alle servers geld dat logrotatie moet worden geconfigureerd voor tomcat logs, logstash logs en elasticsearch logs. De termijn van rotatie zal per omgeving verschillen, zo is op ontwikkel omgeving een termijn van 3 dagen acceptabel maar op de proeftuin zal de periode langer moeten zijn.