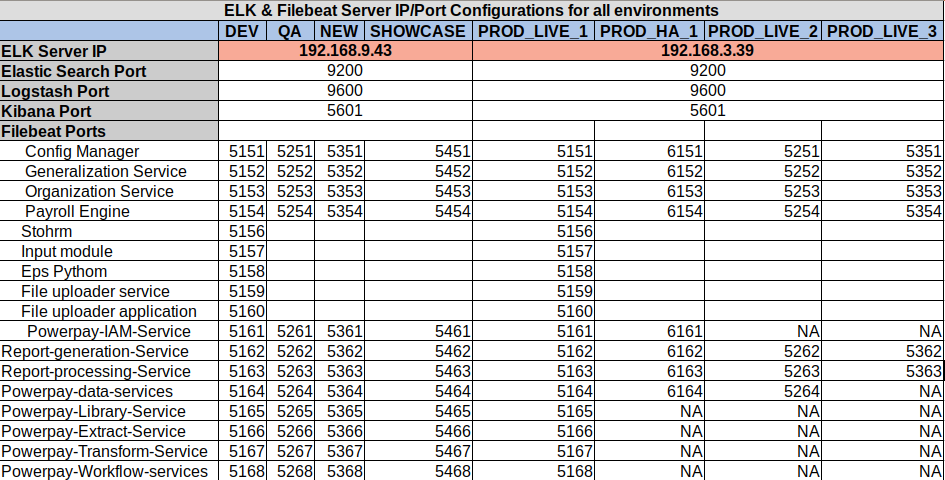
***ELK Server Details:***



\*\*Filebeat ports: Ports enabled in ELK servers for logstash – Filebeat communication

**ELK Installation:**

ELK can be installed through ansible script frombelow repository location:

<https://gitlab.ascent-online.com/powerpay/power-pay-k8s>

1. Login to 192.168.9.16 as root

2. Clone above git repository to a location in above server.

3. cd power-pay-k8s/blob/master/Ansible\_modules/All-in-one/

4. Run ‘ansible-playbook elk-playbook.yml -i All-in-One/inv.ini -e ‘hosts=ELK’

Run elk-playbook.yml file to install elasticsearch, logstash and kibana. Filebeat will be installed as part of application deployment through ansible.

**Related Files & Location:**

* Elasticsearch:

Configuration Files: /*etc/*elasticsearch/elasticsearch.yml

Data Files Path: /var/lib/elasticsearch

Log File Path: */var/log/elasticsearch*

* Logstash:
  + Configuration Files:
    - /*etc/*logstash/pipelines.yml
    - /etc/logstash/conf.d/<env>/ogstash-<app\_name>.conf
  + Log File:
    - /var/log/logstash/logstash-plain.log
* Kibana Configuration files:

*/etc/kibana/kibana.yml*

* Filebeat:

/etc/filebeat/filebeat.yml

***Steps for configuration:***

* *Elasticsearch:*
  + cd /etc/elasticsearch & open elasticsearch.yml for editing.
  + Update below settings if not already present/enabled
    - http.cors.enabled: true
    - http.cors.allow-origin: "\*"
    - network.host: 0.0.0.0
    - http.port: 9200
    - discovery.seed\_hosts: ["0.0.0.0","host1"]
  + Save and close the file.
  + Restart elasticsearch by running ‘sudo systemctl restart elasticsearch.service’
* Logstash:
  + cd /etc/logstash
  + Update pipelines.yml file with required configuration. Refer [https://gitlab.ascent-online.com/powerpay/power-pay-k8s/blob/master/Ansible\_modules/All-in-one/roles/logstash/templates/powerpay-apps/pipelines.yml](https://gitlab.ascent-online.com/powerpay/power-pay-k8s/blob/elk-configurations/Ansible_modules/All-in-one/roles/logstash/templates/powerpay-apps/pipelines.yml)

for sample

* + cd /etc/logstash/conf.d
  + Add logstash conf file for the application. Refer <https://gitlab.ascent-online.com/powerpay/power-pay-k8s/blob/master/Ansible_modules/All-in-one/roles/logstash/templates/powerpay-apps/conf.d/prod_live/logstash-config-manager.conf> or sample.
  + Restart Logstash service by running ‘sudo systemctl restart logstash.serice’

* Kibana:
  + Copy kibana.yml from below location into /etc/kibana
  + Restart Kibana service by running ‘sudo systemctl restart kibana.service’
* Filebeat:
  + Filbeat configuration is automated using ansible scripts. Refer <https://gitlab.ascent-online.com/pnbhat/provisional-deployment-scripts/tree/master/roles/filebeat-app> for scripts.
  + For configuring filebeat for new applications:
    - Add filebeat configuration file into /etc/filebeat/filebeat-<app\_name>.yml
    - Refer <https://gitlab.ascent-online.com/pnbhat/provisional-deployment-scripts/blob/master/roles/filebeat-app/templates/filebeat.yml> for template.
    - Create a systemd service for running app specific filebeat service. Refer <https://gitlab.ascent-online.com/pnbhat/provisional-deployment-scripts/blob/master/roles/filebeat-app/templates/application.service> for systems service script.
    - Restart Filebeat service by running ‘sudo systemctl restart filebeat-<app\_name>.service’

**Restart hierarchy for ELK :**

* Stop Filebeat
* Stop Kibana
* Stop Logstash
* Stop Elasticsearch
* Start Elasticsearch
* Start Logstash
* Start Kibana
* Start Filebeat