\*\*در این داکیومنت قصد داریم تا شمای کلی و کارکردی سرویس الستیک را بررسی نماییم و همچنین با قابلیت Security در این مانیتورینگ بیشتر آشنا شویم و در نهایت با روند کانفیگ کردن Auditbeat و قسمت های مهم آن نیز اشنا میشویم\*\*

**کلاستر الستیک**

در هر کلاستر ELK هر نود یک وظیفه دارند که این وظیفه در کانفیگ فایل انها مشخص میشود که سه عدد از مهمترین آنها به شرح زیر می باشند :

**Master**

این نود وظیفه مدیریت کردن (Coordinate) را دارد.

**Data**

این نود وظیفه ذخیره اطلاعات کلاستر را برعهده دارد.

**Ingest**

این نود در لبه کلاستر قرار دارد و همانند یک گیت وی است و پس از دریافت ریکوئست ها ان را در کلاستر پخش میکند.

**شماتیک سرویس کلاستر الستیک به شرح زیر است :**



طبق شکل بالا سرویس های Legacy که اصطلاحا سرویس های خارج کوبرنتیز هستند از طریق Filebeat لاگ ها را ارسال میکنند و سرویس های K8S که اصطلاحا داخل کوبرنتیز هستند هم از طریق Fluentd لاگ ها را به الستیک ارسال میکنند.

برای جمع اوری اطلاعات امنیتی - زیر ساختی و امنیتی – شبکه ای از Auditbeat و Metricbeat استفاده میکنیم .

با استفاده از Metricbeat میتوان اطلاعات مربوط به مانیتورینگ ریسورس ها را نیز جمع اوری کرد و نمایش داد.

بعداز جمع آوری اطلاعات از ماشین های مورد نظر با ساخت داشبورد های مختلف در کیبانا میتوان سرویس های مد نظر را مانیتور کرد.

**قسمت های مهم کانفیگ فایل Auditbeat:**

در قسمت Auditd module و در قسمت audit\_rules موارد کلی که نیاز به مانیتور کردن آن را داریم در این قسمت اضافه میکنیم و چند نمونه از این موارد در زیر ذکر شدند :

#----------------------------- Auditd module -----------------------------------

audit\_rules: |

-w /var/log/audit/ -k auditlog

-w /etc/inittab -p wa -k init

-w /etc/init.d/ -p wa -k init

-w /etc/init/ -p wa -k init

-w /bin/systemctl -p x -k systemd

-w /etc/systemd/ -p wa -k systemd

-w /etc/selinux/ -p wa -k mac\_policy

-w /var/run/utmp -p wa -k session

-w /var/log/btmp -p wa -k session

-w /etc/login.defs -p wa -k login

-w /etc/securetty -p wa -k login

-w /var/log/lastlog -p wa -k login

-w /var/log/tallylog -p wa -k login

-a always,exit -F arch=b64 -S adjtimex -S settimeofday -S clock\_settime -k time

-w /etc/localtime -p wa -k time

-w /etc/group -p wa -k identity

-w /etc/passwd -p wa -k identity

-w /etc/gshadow -p wa -k identity

-w /etc/shadow -p wa -k identity

-w /etc/auditbeat/auditbeat.yml -p wa -k auditbeat

-w /etc/security/opasswd -p wa -k opasswd

-w /usr/bin/passwd -p x -k passwd\_modification

-w /etc/sudoers -p wa -k action

-w /usr/sbin/groupadd -p x -k group\_modification

-w /usr/sbin/groupmod -p x -k group\_modification

-w /usr/sbin/addgroup -p x -k group\_modification

-w /usr/sbin/useradd -p x -k user\_modification

-w /usr/sbin/usermod -p x -k user\_modification

-w /usr/sbin/adduser -p x -k user\_modification

-a always,exit -F arch=b64 -S open,creat,truncate,ftruncate,openat,open\_by\_handle\_at -F exit=-EACCES -k access

-a always,exit -F arch=b64 -S open,creat,truncate,ftruncate,openat,open\_by\_handle\_at -F exit=-EPERM -k access

-w /etc/pam.d/ -p wa -k pam

-w /etc/security/limits.conf -p wa -k pam

-w /etc/security/pam\_env.conf -p wa -k pam

-w /etc/security/namespace.conf -p wa -k pam

-w /etc/security/namespace.init -p wa -k pam

-w /etc/cron.allow -p wa -k cron

-w /etc/cron.deny -p wa -k cron

-w /etc/cron.d/ -p wa -k cron

-w /etc/cron.daily/ -p wa -k cron

-w /etc/cron.hourly/ -p wa -k cron

-w /etc/cron.monthly/ -p wa -k cron

-w /etc/cron.weekly/ -p wa -k cron

-w /etc/crontab -p wa -k cron

-w /var/spool/cron/crontabs/ -k cron

-w /etc/ssh/sshd\_config -k sshd

-w /root/.ssh/authorized\_keys -k ssh\_files

-a always,exit -F arch=b64 -S execve,execveat -k exec

در تب output میباست اطلاعات مربوط به سرور الستیک به همراه یوزر و پسورد را وارد نماییم :

#================================ Outputs ======================================

#

# Configure what output to use when sending the data collected by the beat.

#

output.elasticsearch:

hosts: ["http://es01:9200"]

username: "elastic"

password: "elastic"

در تب کیبانا نیز اطلاعات مربوط به Url سرور کیبانا و نوع پروتکل را وارد میکنیم :

#============================== Kibana =====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.

# This requires a Kibana endpoint configuration.

setup.kibana:

# Kibana Host

# Scheme and port can be left out and will be set to the default (http and 5601)

# In case you specify and additional path, the scheme is required: http://localhost:5601/path

# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601

host: "kib01:5601"

# Optional protocol and basic auth credentials.

protocol: "http"

موارد ذکر شده در قسمت کانفیگ فایل همه به صورت تستی وارد و جای گذاری شدند.