**GRAYLOG - Firewall**

**Equipe**

**CENTRALIZAÇÃO DE LOGS DE ACESSO AOS SERVIDORES, UTLIZANDO O GRAYLOG**

Este projeto tem como objetivo implementar a ferramenta GrayLog como solução para centralizar os logs de acesso do firewall fortigate FGT-600E da rede da Prefeitura Municipal de Cuiabá. GrayLog é um software livre e de código aberto que tem como finalidade de centralizar, consolidar, indexar e analisar os logs gerados em máquinas Windows. Ele permite gerar gráficos baseados em eventos criados pelo. Opcionalmente, sua interface de entrada pode ser integrada com colecionadores de log diferente, tais como rsyslog, syslog-ng, logstash e nxlog. Ele também possui um painel grande e fácil de entender baseado em web com vistas pré-definidas para acesso rápido.

O GrayLog possui 4 compontenes, sendo eles:

* MongoDB - armazena as configurações e informações do servidor
* ElasticSearch - armazena as mensagens de log e oferece uma facilidade de busca de logs.
* GrayLog Server- Log analisador, é coletar os registros de várias entradas.
* GrayLog Web = fornece-lhe o portal baseado na web para gerenciar os logs.

**Porque utilizar o Graylog:**

O Graylog permitirá que a DTI possa monitorar e armazenar por um período de 3 meses o que os usuários acessaram na internet, tornando um recurso que o administrador de rede possui para descobrir os acessos indevidos. Além do mais, GrayLog é fácil de configurar, e requer pouca manutenção.

**Objetivos inicial do projeto:**

|  |
| --- |
| **Implantação do servidor Graylog** |
| **Ativar geração de logs no firewall fortinet** |
| **Enviar os logs do firewall para o servidor GrayLog** |
| **Gerenciar as entradas dos Logs no Graylog Server** |
| **Visualizar os logs gerados** |

**Etapas do projeto:**

|  |  |  |
| --- | --- | --- |
| **Etapas** | **Atividades executadas** | **Status** |
| 1-Implantação do servidor Graylog | - Levantar uma máquina CentOS 7  - Instalar os pré-requisitos: Java  - Instalar o MongoDB  - Instalar o ElasticSearch  - Instalar o GrayLog Server  - Instalar o GrayLog Web | Concluído |
| 2-Configuração do GrayLog | - Configurar o MongoDB  - Configurar o ElasticSearch  - Configurar o GrayLog Server  - Configurar o GrayLog Web | Concluído |
| 3-Configuração do firewall | - Configurar o fortigate para enviar logs para o servidor.  - Visualizar os logs gerados | Concluído |
| 5-Relatórios | - Homologação do projeto  - Criação de relatórios periódicos | Concluído |

**Processo de Implantação e Configuração do Servidor Graylog, utilizando uma VM Oracle Linux 8:**

**Java**

O ElasticSearch e Graylog é baseado em java, logo é necessário instalar o java com o comando

# yum update && yum -y install java-1.8.0-openjdk-headless.x86\_64

**ElasticSearch**

Instalou-se o ElasticSearch versão 7.14 e realizou-se os seguintes passos:

Importar a chave GPG.

rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

Adicionou repositório ElasticSearch. - */etc/yum.repos.d/*elasticsearch.repo

[elasticsearch-7.x]

name=Elasticsearch repository for 7.x packages

baseurl=https://artifacts.elastic.co/packages/oss-7.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

Instalou a versão mais recente usando o comando yum

yum install elasticsearch-oss

Editar o arquivo de configuração: nano /etc/elasticsearch/elasticsearch.yml

# nano /etc/elasticsearch/elasticsearch.yml

cluster.name: graylog

node.name: ${HOSTNAME}

network.host: 0.0.0.0

http.port: 9200

discovery.zen.ping.unicast.hosts: ["resflorcerrado.cuiaba.mt.gov.br", "coxipodaponte.cuiaba.mt.gov.br", "jdcomodoro.cuiaba.mt.gov.br”]

Configurou o Elasticseach para iniciar durante a inicialização do sistema.

systemctl daemon-reload

systemctl enable elasticsearch.service

systemctl restart elasticsearch.service

Checar o status do Elasticsearch através do curl:

curl http://resflorcerrado.cuiaba.mt.gov.br:9200

Desabilitar o firewall e SELinux para todas as maquinas.

systemctl disable firewalld

nano /etc/sysconfig/selinux

SELINUX=disabled

**Instalar o MongoDB**

Adicionou-se as seguintes informações sobre o sistema de repositório para instalar MongoDB 5 usando o yum. Editar arquivo em: nano */etc/yum.repos.d/mongodb-org-5.0.repo*

[mongodb-org-5.0]

name=MongoDB Repository

baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/5.0/x86\_64/

gpgcheck=1

enabled=1

gpgkey=https://www.mongodb.org/static/pgp/server-5.0.asc

Instalou-se MongoDB usando o seguinte comando.

yum update && yum install -y mongodb-org

Configuração do MongoDB , crie os diretórios:

mkdir -p /var/lib/mongo

mkdir -p /var/log/mongodb

mkdir -p /data/db

Configuração do MongoDB , permissões do usuário mongod:

chown -R mongod:mongod /var/lib/mongo

chown -R mongod:mongod /var/log/mongodb

Inicou-se o serviço MongoDB e habilitou-se para iniciar automaticamente durante o sistema start-up.

systemctl daemon-reload

systemctl enable mongod

systemctl start mongod

Editar o arquivo /etc/mongod.conf e adicionar os parâmetros para todos as maquinas jd8abril.cuiaba.mt.gov.br, jdpauliceia.cuiaba.mt.gov.br e rescoxipones.cuiaba.mt.gov.br.

# network interfaces

net:

port: 27017

bindIp: 127.0.0.1,jd8abril.cuiaba.mt.gov.br

. . .

replication:

replSetName: "rs0"

. . .

Criar banco de dados para o graylog no terminal digite:

mongo

use graylog;

db.createUser( { user: "mongo\_admin", pwd: "graylog", roles: [ { role: "root", db: "admin" } ] } )

**Instalar o GrayLog**

Digite no terminal

rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-4.1-repository\_latest.rpm

yum update && yum -y install java-1.8.0-openjdk-headless.x86\_64 graylog-server

**Configuração do GrayLog**

Gerar a password\_secret basta executar o comando:

pwgen -N 1 -s 96

GehjzryuwhTLTLBsP5TDsXBk3jE8BBTlsbnsApk4L8TG7KtLXM4efx1XzJwS51egffsuYOvgnxJu4K2jygoAOuLUBDgn7ITp

Gerar a root\_password\_sha2 basta executar o comando:

echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1

Editar arquivo de configuração /etc/graylog/server/server.conf

is\_master = true

password\_secret = [gerada anteriormente]

root\_password\_sha2 = [gerada anteriormente]

root\_timezone = America/Cuiaba

http\_bind\_address = jd8abril.cuiaba.mt.gov.br:9000

http\_publish\_uri = http://jd8abril.cuiaba.mt.gov.br:9000/

elasticsearch\_hosts = http://resflorcerrado.cuiaba.mt.gov.br:9200,http://coxipodaponte.cuiaba.mt.gov.br:9200,http://jdcomodoro.cuiaba.mt.gov.br:9200

elasticsearch\_shards = 3

mongodb\_uri = mongodb://mongo\_admin:graylog@jd8abril.cuiaba.mt.gov.br:27017,jdpauliceia.cuiaba.mt.gov.br:27017,rescoxipones.cuiaba.mt.gov.br:27017/graylog?replicaSet=rs0

Agora basta iniciar o servidor do Graylog:

# systemctl daemon-reload

# systemctl enable graylog-server

# systemctl start graylog-server

**Instalar o HAProxy**

Digitar no terminal.

yum update && yum install haproxy

Edite o arquivo de configuração e insira os blocos

vim /etc/haproxy/haproxy.cfg

frontend graylog\_http

bind \*:80

option forwardfor

http-request add-header X-Forwarded-Host %[req.hdr(host)]

http-request add-header X-Forwarded-Server %[req.hdr(host)]

http-request add-header X-Forwarded-Port %[dst\_port]

acl is\_graylog hdr\_dom(host) -i -m str graylog.example.org

use\_backend graylog

backend graylog

description The Graylog Web backend.

balance roundrobin

option httpchk HEAD /api/system/lbstatus

http-request set-header X-Graylog-Server-URL http://graylog.example.org/

server graylog1 jd8abril.cuiaba.mt.gov.br:9000 maxconn 20 check

server graylog2 jdpauliceia.cuiaba.mt.gov.br:9000 maxconn 20 check

server graylog3 rescoxipones.cuiaba.mt.gov.br:9000 maxconn 20 check

log-forward syslog-lb

#bind :::15514 # Listen on TCP IPv4/IPv6

dgram-bind :::15514 # Listen on UDP IPv4/IPv6

# load balance messages on 4 udp syslog servers

log jd8abril.cuiaba.mt.gov.br:15514 format rfc5424 sample 1:3 local0 info

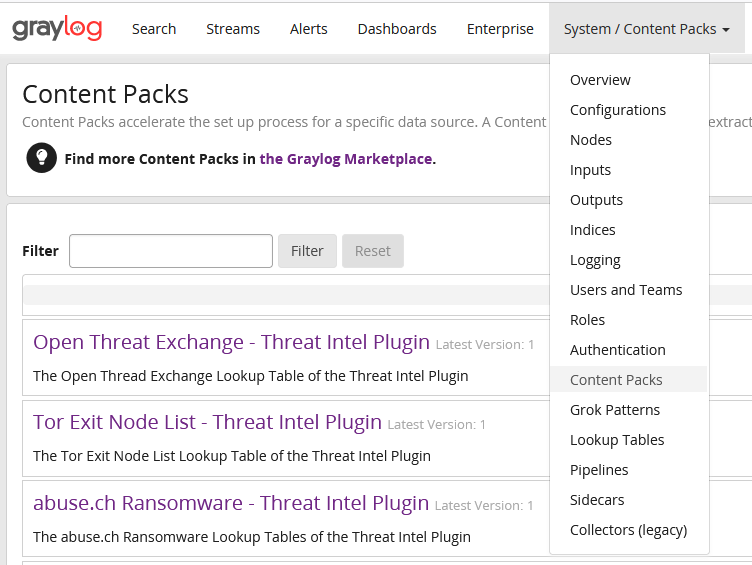
log jdpauliceia.cuiaba.mt.gov.br:15514 format rfc5424 sample 1:3 local0 info

log rescoxipones.cuiaba.mt.gov.br:15514 format rfc5424 sample 1:3 local0 info

**Instalar o ContentPacks**

Baixar no site.

https://github.com/pfitchie/graylog3.Fortigate6xContentPack

Importar o arquivo em System/Content Packs :  
  


Clicar em Upload e enviar o conteúdo baixado:  
