Servizi

I servizi presenti sul server sono i seguenti:

1. MongoDb
2. Elastisearch
3. Graylog-Server

```
systemctl status mongodb.service
systemctl status elasticsearch.service
systemctl status graylog-server
```

Web manager è http://graylog.bo.priv:9000/

Configurazioni

Il file di configurazione per il GrayLog è
`/etc/graylog/server/server.conf`

Monitorare Server Linux

Installare sul server che si desidera mandare i log, RSYSLOG. Creare un file rsyslog.conf in /etc/rsyslog.d con il seguente contenuto:

```
*.* @10.17.61.115;1024;RSYSLOG_SyslogProtocol23Format
*.* @@10.17.61.115:1024;RSYSLOG_SyslogProtocol23Format
```

Servono per il traffico tcp e udp. Richiesta nella porta 1024 del server.

Modificare il file /etc/rsyslog.conf e modificare come il seguente:

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

###############
#### RULES ####
###############

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
#*.*;auth,authpriv.none         -/var/log/syslog
#cron.*                         /var/log/cron.log
#daemon.*                       -/var/log/daemon.log
#kern.*                         -/var/log/kern.log
#lpr.*                          -/var/log/lpr.log
#mail.*                         -/var/log/mail.log
#user.*                         -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
#mail.info                      -/var/log/mail.info
#mail.warn                      -/var/log/mail.warn
#mail.err                       /var/log/mail.err

#
# Some "catch-all" log files.
#
*.=debug;\
        auth,authpriv.none;\
```

```
#       news.none;mail.none     -/var/log/debug
*.=info;*.=notice;*.=warn;\
        auth,authpriv.none;\
#       cron,daemon.none;\
#       mail,news.none          -/var/log/messages
```

Riavviare il servizio rsyslog. `service rsyslog restart`

Sul web di Graylog, aggiungere un input per la seguente richiesta. Se esiste già. Non c'è bisogno di fare nulla. Altrimenti andare su :

System/Indeces⇒Inputs⇒Select Input⇒Syslog TCP poi Launch new Input. Nella schermata seguente precisare il nodo e la porta. Nel caso nostro 1024.

Retention

Andare su System/Indeces⇒Indices per editare l'indice secondo le preferenze. Qui si puo specificare la retention.

SSH

Per avere delle informazioni più leggibili in ssh auth configurare come segue.

Aggiungere in .ssh/authorized_keys la variabile SSH_USER in tutti i server

```
environment="SSH_USER=Marvin Pascale" ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCYVWGspW9NMvKPM5XgQOcMvEyHt57yu7aXVLIpZxXqfHtRDrrYxXREKxKfUM4mu3N7V6
TkpikzuwGD5IOC9mVzxzrqx8c3ORfXlX+0VIgWr4l5Q3u9vU2QOcWDsO1B7ozlZ96JhafGct6V9Igl90dMmXdO6i0uqP1ksUHL
VzadCoxvcix4RZN6vU2BIyAS0rvJtUsuE45IZh+izIIphi0k1fp5XLq+dDC9ZDdHukWfT8rCsqk7hRJC2qUTFoXKpHeqG/OYYj
iA8iRV6G+WPP5U3aFn2h8mYpLvsa6d4UrLUdKQIpTMOKr1K75sPUJ7Zccy32boxwEBlExGo826remb mpascale@3di.it
```

Creare lo script sshrc /etc/ssh/sshrc

```
ip=`echo $SSH_CONNECTION | cut -d " " -f 1`
logger -t ssh-wrapper $SSH_USER login from $ip
```

Modificare /etc/ssh/sshd_config con `PermitUserEnvironment yes`

Monitorare Server Windows

Installare nxlog dal sito https://nxlog.co/products/nxlog-community-edition/download. Modificare il seguente file C:\Program Files (x86)\nxlog\conf\nxlog.conf

```
<Extension _gelf>

     Module xm_gelf
</Extension>

<Input In>
    Module    im_msvistalog
        ReadFromLast FALSE
        SavePos     FALSE
    Query <QueryList> \
        <Query Id="0"> \
    <Select Path="Security"> *[System[(EventID=4624) and TimeCreated[timediff(@SystemTime)
&lt;=86400000]]] and *[EventData[Data[@Name='logontype'] and (Data='10')]] </Select> \
    </Query> \
    </QueryList>
</Input>

<Output out>
    Module om_tcp
    Host    10.17.61.115
    Port    12201
    OutputType    GELF_TCP
</Output>

<Route 1>
    Path    In => out
</Route>
```

La porta 12201 è casuale. Stare attenti che a volte l'input sul web non funziona con certe porte. Quindi cambiare. Dal web andare su System⇒Inputs⇒Select Input⇒GELF TCP e poi Launch new input. Dovrebbe già esistere. Se no, aggiungerlo.