# Architektur

# 

# Server

Folgende Server wurden für den Elasticsearch Cluster verwendet:

|  |  |
| --- | --- |
| **Hostname** | **Funktion** |
| VSAT-LOG-DAT1.servers.emea.dir | ELKCLUSTER – Data Node 1 |
| VSAT-LOG-DAT2.servers.emea.dir | ELKCLUSTER – Data Node 2 |
| VSAT-LOG-MAS1.servers.emea.dir | ELKCLUSTER – Master Node 1 |
| VSAT-LOG-MAS2.servers.emea.dir | ELKCLUSTER – Master Node 2 |
| VSAT-LOG-MAS3.servers.emea.dir | ELKCLUSTER – Master Node 3 |
| VSAT-LOG-STASH1.servers.emea.dir (ALIAS: log.services.emea.dir) | LOGSTASH |

# Ports

Folgende Ports werden derzeit verwendet:

|  |  |  |
| --- | --- | --- |
| **Hostname** | **Port** | **Funktion** |
| VSAT-LOG-MAS[*1-3*].servers.emea.dir | 9200 | Elasticsearch REST API (Extern) |
| VSAT-LOG-DAT[*1-2*].servers.emea.dir | 9200 | Elasticsearch REST API (Intern) |
| VSAT-LOG-MAS[*1-3*].servers.emea.dir | 9300 | Elasticsearch Kommunikation (Intern) |
| VSAT-LOG-DAT[*1-2*].servers.emea.dir | 9300 | Elasticsearch Kommunikation (Intern) |
| VSAT-LOG-MAS[*1-3*].servers.emea.dir | 5601 | Web Interface (Extern) |
| log.services.emea.dir | 15102 | Logstash Lumberjack Input (für forwarder) |

# URLs

Folgende Adressen sind im Cluster relevant:

|  |  |
| --- | --- |
| **Adresse** | **Funktion** |
| http://vsat-log-mas[*1-3*].servers.emea.dir:5601/app/kibana | Kibana Web Interface |
| http://vsat-log-mas[*1-3*].servers.emea.dir:5601/app/marvel | Marvel Web Interface |
| http://vsat-log-mas[*1-3*].servers.emea.dir:9200/ | Elasticsearch REST Interface |

# Firewall-Freischaltungen

Folgende Firewall-Freischaltungen sind zum Funktionieren des Clusters erforderlich:

iptables …

|  |  |  |
| --- | --- | --- |
| **Hostname** | **Regel** |  |
| VSAT-LOG-STASH1 | -A INPUT -p tcp -s 172.17.64.193 --dport 15102 -j ACCEPT  -A INPUT -p tcp -s 172.18.64.145 --dport 15102 -j ACCEPT  -A INPUT -p tcp -s 172.19.64.145 --dport 15102 -j ACCEPT  -A INPUT -p tcp -s 172.17.64.84 --dport 15102 -j ACCEPT  -A INPUT -p tcp -s 172.17.64.83 --dport 15102 -j ACCEPT  -A INPUT -p tcp -s 172.17.64.206 --dport 15102 -j ACCEPT  -A INPUT -p tcp -s 172.17.64.102 --dport 15102 -j ACCEPT  -A INPUT -p tcp -s 172.17.64.247 --dport 15102 -j ACCEPT | Logstash Input |
| VSAT-LOG-MAS[*1-3*] | -A INPUT -p tcp --dport 9200 -j ACCEPT  -A INPUT -p tcp --dport 5601 -j ACCEPT | REST-Interface Kibana-GUI |
| VSAT-LOG-MAS[*1-3*] VSAT-LOG-DAT[*1-2*] | -A INPUT -p tcp -s 172.17.64.24 --dport 9300 -j ACCEPT  -A INPUT -p tcp -s 172.17.64.32 --dport 9300 -j ACCEPT  -A INPUT -p tcp -s 172.17.64.51 --dport 9300 -j ACCEPT  -A INPUT -p tcp -s 172.17.64.98 --dport 9300 -j ACCEPT  -A INPUT -p tcp -s 172.17.64.99 --dport 9300 -j ACCEPT  -A INPUT -p tcp -s 172.17.64.108 --dport 9300 -j ACCEPT | Cluster-Interne Kommunikation |

# Bereits über Forwarder angebunden Clients

Folgende Hosts sind bereits über den logstash-forwarder an Logstash angebunden:

|  |
| --- |
| **Hostname** |
| vsat-gitlab |
| vsel-icinga |
| vsen-icinga |
|  |