INTEGRATED MONITORING PORTAL FOR LATIN AMERICAN NRENs

Tiago Monsores, Lead Network Engineer
What is RedCLARA?

RedCLARA is the result of cooperation between Latin American countries to create a high-capacity network dedicated to research and education.
What is RedCLARA?

We strengthen the development of science, education, culture and innovation in Latin America, through the innovative use of networks, infrastructure and advanced information technologies.
What is RedCLARA?

Today this cooperation has 9 countries totaling 15,759,828 km² of territory. This vast territory must be covered by national networks, making it possible to reach the most diverse regions.
Network characteristics

- High capacity: all backbone links are +100Gbps
- Predictability: traffic flows through a coherent path
- Security: MANRS participant with all 4 actions implemented + 100% score
- Robust monitoring
NEG Systems

- Grafana
  - Network traffic monitoring
- chronograf
  - Virtual machines monitoring
- graylog
  - Management of log messages
- ElastiFlow
  - Collects and analyzes network flows
- Oxidized
  - Configuration backup and management

- ZABBIX
  - Monitoring and alerting system
- Pushover
  - Push notifications system
- TACACSGUI
  - User authentication, and command authorization and accounting
- ROUTINATOR
  - RPKI validation system
One of the most requested features from RedCLARA members was network visibility. Network monitoring was present, but information was internal.
Cooperación LatinoAmericana de Redes Avanzadas

Architecture

- **Telegraf**
  - Agent for collecting metrics

- **InfluxDB**
  - Time Scale Database (TSDB)

- **Zabbix**
  - Monitoring tool

- **TimescaleDB**
  - Time Scale Database (TSDB)

- **Logstash**
  - Agent for collecting flows

- **Kibana**
  - Flow information interface

- **Elasticsearch**
  - Database and search engine

- **TACACS**
  - AAA

- **WebSSH**
  - Web based SSH client

- **Grafana**
  - Metrics information interface

- **Integrated Monitoring Portal**
Graphical Interface and Authentication

- Graphical interface built with Drupal
- Drupal is an open source Content Management System (CMS)
- Authentication uses Shibboleth for federated login
- Created by SEG (System Engineering Group)
Traffic and BGP Monitoring

- SNMP metrics collected with Telegraf using a polling time of 30 seconds
- Latency measured with IP SLA
- Data is stored in InfluxDB
- Availability and Alerts provided by Zabbix
- Dashboards built with Grafana

TechEX2023
Network Flows Monitoring

- Netflow v9 is configured on the routers
- Only 0.01% of the packets are sampled
- Flows are exported to Logstash
- Data is enriched and sent to Elasticsearch
- Dashboards are made for Kibana and are part of ElastiFlow
### Services (bits/s)

<table>
<thead>
<tr>
<th>Service</th>
<th>Bytes</th>
<th>Packets</th>
<th>Flow Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethtool</td>
<td>8.904Gbits/s</td>
<td>0bits/s</td>
<td>0bits/s</td>
</tr>
<tr>
<td>rsync (TCP/873)</td>
<td>0bits/s</td>
<td>0bits/s</td>
<td>0bits/s</td>
</tr>
<tr>
<td>https (TCP)</td>
<td>8.001MBits/s</td>
<td>0bits/s</td>
<td>0bits/s</td>
</tr>
<tr>
<td>https (UDP/443)</td>
<td>0bits/s</td>
<td>0bits/s</td>
<td>0bits/s</td>
</tr>
<tr>
<td>ldoms-ma...</td>
<td>2.1Mbits/s</td>
<td>0bits/s</td>
<td>0bits/s</td>
</tr>
<tr>
<td>ssh IT</td>
<td>768.647KBits/s</td>
<td>0bits/s</td>
<td>0bits/s</td>
</tr>
<tr>
<td>ipsec-nat</td>
<td>4.163MBits/s</td>
<td>0bits/s</td>
<td>0bits/s</td>
</tr>
<tr>
<td>http (TCP)</td>
<td>3.387MBits/s</td>
<td>0bits/s</td>
<td>0bits/s</td>
</tr>
</tbody>
</table>

### Top Clients

<table>
<thead>
<tr>
<th>Client</th>
<th>Bytes</th>
<th>Packets</th>
<th>Flow Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>147.186.117.68</td>
<td>59.74MB</td>
<td>70,070</td>
<td>1,978</td>
</tr>
<tr>
<td>147.186.117.71</td>
<td>88.27MB</td>
<td>60,635</td>
<td>1,821</td>
</tr>
<tr>
<td>2001:638:700::f0c3:1fe</td>
<td>14.56MB</td>
<td>10,196</td>
<td>298</td>
</tr>
<tr>
<td>193.206.153.244</td>
<td>13.76MB</td>
<td>9,757</td>
<td>228</td>
</tr>
<tr>
<td>2001:638:700::f0c3:1fd</td>
<td>13.26MB</td>
<td>9,278</td>
<td>295</td>
</tr>
<tr>
<td>141.34.192.140</td>
<td>12.34MB</td>
<td>9,000</td>
<td>296</td>
</tr>
<tr>
<td>2001:638:700::f0c3:1fa</td>
<td>12.26MB</td>
<td>8,973</td>
<td>283</td>
</tr>
<tr>
<td>141.34.192.138</td>
<td>12.80MB</td>
<td>8,984</td>
<td>243</td>
</tr>
<tr>
<td>141.34.192.142</td>
<td>12.70MB</td>
<td>8,904</td>
<td>247</td>
</tr>
<tr>
<td>2001:638:700::f0c3:1fa</td>
<td>12.63MB</td>
<td>8,830</td>
<td>207</td>
</tr>
</tbody>
</table>

**Total:** 567,715 packets, 40,328 flow records

### Top Servers

<table>
<thead>
<tr>
<th>Server</th>
<th>Bytes</th>
<th>Packets</th>
<th>Flow Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.17.30.65</td>
<td>373.994MB</td>
<td>262,572</td>
<td>7,099</td>
</tr>
<tr>
<td>200.12.18.020-65</td>
<td>328.533MB</td>
<td>228,774</td>
<td>5,621</td>
</tr>
<tr>
<td>200.236.31.10</td>
<td>11.058MB</td>
<td>7,731</td>
<td>110</td>
</tr>
<tr>
<td>200.236.31.13</td>
<td>2.284MB</td>
<td>1,007</td>
<td>123</td>
</tr>
<tr>
<td>200.144.255.251</td>
<td>1.524MB</td>
<td>1,323</td>
<td>747</td>
</tr>
<tr>
<td>129.247.239.1</td>
<td>1.008MB</td>
<td>768</td>
<td>220</td>
</tr>
<tr>
<td>2001:638:700::f0c3:1fa</td>
<td>718.509KB</td>
<td>10,151</td>
<td>5,555</td>
</tr>
<tr>
<td>200.236.31.8</td>
<td>703.125KB</td>
<td>480</td>
<td>59</td>
</tr>
<tr>
<td>129.247.239.11</td>
<td>513.066KB</td>
<td>586</td>
<td>494</td>
</tr>
<tr>
<td>200.17.30.43</td>
<td>470.584KB</td>
<td>388</td>
<td>310</td>
</tr>
</tbody>
</table>

**Total:** 567,715 packets, 40,328 flow records
The WeatherMap shows current backbone traffic and latency.

- It has been built with Zabbix.
- General view for backbone circuit outages.
WebSSH

- Built with WebSSH (https://github.com/huashengdun/webssh)
- User authentication, command authorization and accounting done by TACACSGUI
- Only ping, traceroute and a set of show commands are allowed
<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Spk</th>
<th>AS</th>
<th>MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
<th>Up/Down</th>
<th>St/FxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>198.32.252.205</td>
<td>0</td>
<td>2000000</td>
<td>378000</td>
<td>383966</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>1w5d</td>
<td>1592</td>
</tr>
<tr>
<td>198.71.45.210</td>
<td>0</td>
<td>11527</td>
<td>222800</td>
<td>220434</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>5d15h</td>
<td>17819</td>
</tr>
<tr>
<td>200.0.204.157</td>
<td>0</td>
<td>11360</td>
<td>159836</td>
<td>956779</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>2d27h</td>
<td>147</td>
</tr>
<tr>
<td>200.0.204.178</td>
<td>0</td>
<td>1797</td>
<td>140622</td>
<td>736188</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>3w0d</td>
<td>3</td>
</tr>
<tr>
<td>200.0.204.214</td>
<td>0</td>
<td>1916</td>
<td>371949</td>
<td>930739</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>15w3d</td>
<td>687</td>
</tr>
<tr>
<td>200.0.205.2</td>
<td>0</td>
<td>27750</td>
<td>493856</td>
<td>1077149</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>15w3d</td>
<td>4321</td>
</tr>
<tr>
<td>200.0.205.3</td>
<td>0</td>
<td>27750</td>
<td>81229916</td>
<td>1078545</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>8w2d</td>
<td>20649</td>
</tr>
<tr>
<td>200.0.205.4</td>
<td>0</td>
<td>27750</td>
<td>156409</td>
<td>1077838</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>15w3d</td>
<td>0</td>
</tr>
<tr>
<td>200.0.205.5</td>
<td>0</td>
<td>27750</td>
<td>178904</td>
<td>1077838</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>3w0d</td>
<td>338</td>
</tr>
<tr>
<td>200.0.205.7</td>
<td>0</td>
<td>27750</td>
<td>156256</td>
<td>1080550</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>10w3d</td>
<td>0</td>
</tr>
<tr>
<td>200.0.205.8</td>
<td>0</td>
<td>27750</td>
<td>163157</td>
<td>1077838</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>15w3d</td>
<td>73</td>
</tr>
<tr>
<td>200.0.205.9</td>
<td>0</td>
<td>27750</td>
<td>165342</td>
<td>1077709</td>
<td>4666047</td>
<td>0</td>
<td>0</td>
<td>5d21h</td>
<td>93</td>
</tr>
</tbody>
</table>
• eduroam information is collected from logs
• Logs are ingested to ELK Stak
• Custom dashboards have been created to output the information
Brazil users authentications:
1,094,568 Authentications

Foreign authentications in Brazil:
426,724 Authentications

Countries visited by Brazil users:
- Outside LATAM (98.75%)
- Argentina (0.6%)
- Brazil
- Chile
- Colombia
- Costa Rica
- Ecuador
- Mexico
- Uruguay
- Outside LATAM

Foreign users authenticated in Brazil (by Country):
- Portugal (25.41%)
- Germany (11.13%)
- United Kingdom (9.13%)
- France (8.03%)
- Spain (5.86%)
- Italy (4.06%)
- Sweden (3.67%)
- Netherlands (3.05%)
- Austria (2.04%)
- Switzerland (1.26%)
- Others (4.01%)
- Missing
Bienvenido a IMP RedCLARA
QUESTIONS?