NAME

ralabel.conf – ralabel resource file.

SYNOPSIS

ralabel.conf

DESCRIPTION

This configuration is a ralabel(1) configuration file.

The concept is to provide a number of labeling strategies with configuration capabilities for each of the labelers. This allows the user to specify the order of the labeling, which is provided to support hierarchical labeling.

Here is a valid and simple configuration file. It doesn't do anything in particular, but it is one that is used at some sites.

Supported Labeling Strategies

Addresss Based Classification

Address based classifications involve building a patricia tree that we can hang labels against. The strategy is to order the address label configuration files, to develop a hierarchical label scheme.

IANA IPv4 and IPv6 Address Classification Labeling

RALABEL_IANA_ADDRESS

The type of IP network address can be used by many analysis programs to make decisions. While IANA standard classifications don't change, this type of classification should be extendable to allow local sites to provide additional labeling capabilities.

RALABEL_IANA_ADDRESS=yes
RALABEL_IANA_ADDRESS_FILE="/usr/local/argus/iana-address-file"

Addresss Based Country Code Classification

RALABEL_ARIN_COUNTRY_CODES

Address based country code classification leverages the feature where ra* clients cant print country codes for the IP addresses that are in a flow record. Country codes are generated from the ARIN delegated address space files. Specify the location of your DELEGATED_IP file here, or in your .rarc file (which is default).

Unlike the GeoIP based country code labeling, these codes can be sorted filtered and aggregated, so if you want to do that type of operations with country codes, enable this feature here.

RALABEL_ARIN_COUNTRY_CODES=yes
RA_DELEGATED_IP="/usr/local/argus/delegated-ipv4-latest"

BIND Based Classification

RALABEL_BIND_NAME

BIND services provide address to name translations, and these reverse lookup strategies can provide FQDN labels, or domain labels that can be added to flow. The IP addresses that can be are synonomous and result in labeling all three IP addresses.

Use this strategy to provide transient semantic enhancement based on ip address values.

RALABEL_BIND_NAME="all"

Port Based Classification

RALABEL_IANA_PORT

Port based classifications involves simple assignment of a text label to a specific port number. While IANA standard classifications are supported throught the Unix /etc/services file assignments, and the basic "src port" and "dst port" ra* filter schemes, this scheme is used to enhance/modify that labeling strategy. The text associated with a port number is placed in the metadata label field, and is searched using the regular expression searching strategies that are available to label matching.

Use this strategy to provide transient semantic enhancement based on port values.

RALABEL_IANA_PORT=yes
RALABEL_IANA_PORT_FILE="/usr/local/argus/iana-port-numbers"

Flow Filter Based Classification

Flow filter based classification uses the standard flow filter strategies to provide a general purpose labeling scheme. The concept is similar to racluster()'s fall through matching scheme. Fall through the list of filters, if it matches, add the label. If you want to continue through the list, once there is a match, add a "cont" to the end of the matching rule.

RALABEL_ARGUS_FLOW

RALABEL_ARGUS_FLOW=yes
RALABEL_ARGUS_FLOW_FILE="/usr/local/argus/argus-flow-file"

GeoIP Based Labeling

The labeling features can use the databases provided by MaxMind using the GeoIP LGPL libraries. If your code was configured to use these libraries, then enable the features here.

GeoIP provides a lot of support for geo-location, configure support by enabling a feature and providing the appropriate binary data files. ASN reporting is done from a separate set of data files, obtained from MaxMind.com, and so enabling this feature is independent of the traditional city data available.

RALABEL_GEOIP_ASN

Labeling data with Origin ASN values involves simply indicating the desire, and the filename for the database of ASN numbers.

RALABEL_GEOIP_ASN=yes
RALABEL_GEOIP_ASN_FILE="/usr/local/share/GeoIP/GeoIPASNum.dat"

RALABEL_GEOIP_CITY

Data for city relevant data is enabled through enabling and configuring the city database support. The types of data available are:

country_code, country_code3, country_name, region, city, postal_code,
latitude, longitude, metro_code, area_code and continent_code.
time_offset is also available.

The concept is that you should be able to add semantics for any IP address that is in the argus record. Support addresses are:

saddr, daddr, inode

The labels provided will be tagged as:

```
scity, dcity, icity
```

To configure what you want to have placed in the label, use the list of objects, in whatever order you like, as the RALABLE_GEOPIP_CITY string using these keywords:

```
cco   - country_code
cco3  - country_code3
cname - country_name
reg   - region
city  - city
pcode - postal_code
lat   - latitude
long  - longitude
metro - metro_code
area  - area_code
cont  - continent_code
off   - GMT time offset
```

Working examples could be:

```
RALABEL_GEOIP_CITY="saddr,daddr:lat/lon"
RALABEL_GEOIP_CITY="*:city,region,cname,lat,lon"
```

RALABEL_GEOIP_CITY="saddr,daddr,inode:lat,lon"
RALABEL_GEOIP_CITY_FILE="/usr/local/share/GeoIP/GeoIPCity.dat"

COPYRIGHT

Copyright (c) 2000-2014 QoSient All rights reserved.

SEE ALSO

ralabel(1)