DNS Statistics Collector

Duane Wessels
The Measurement Factory/ISC/CAIDA
wessels@measurement-factory.com

October 1, 2004

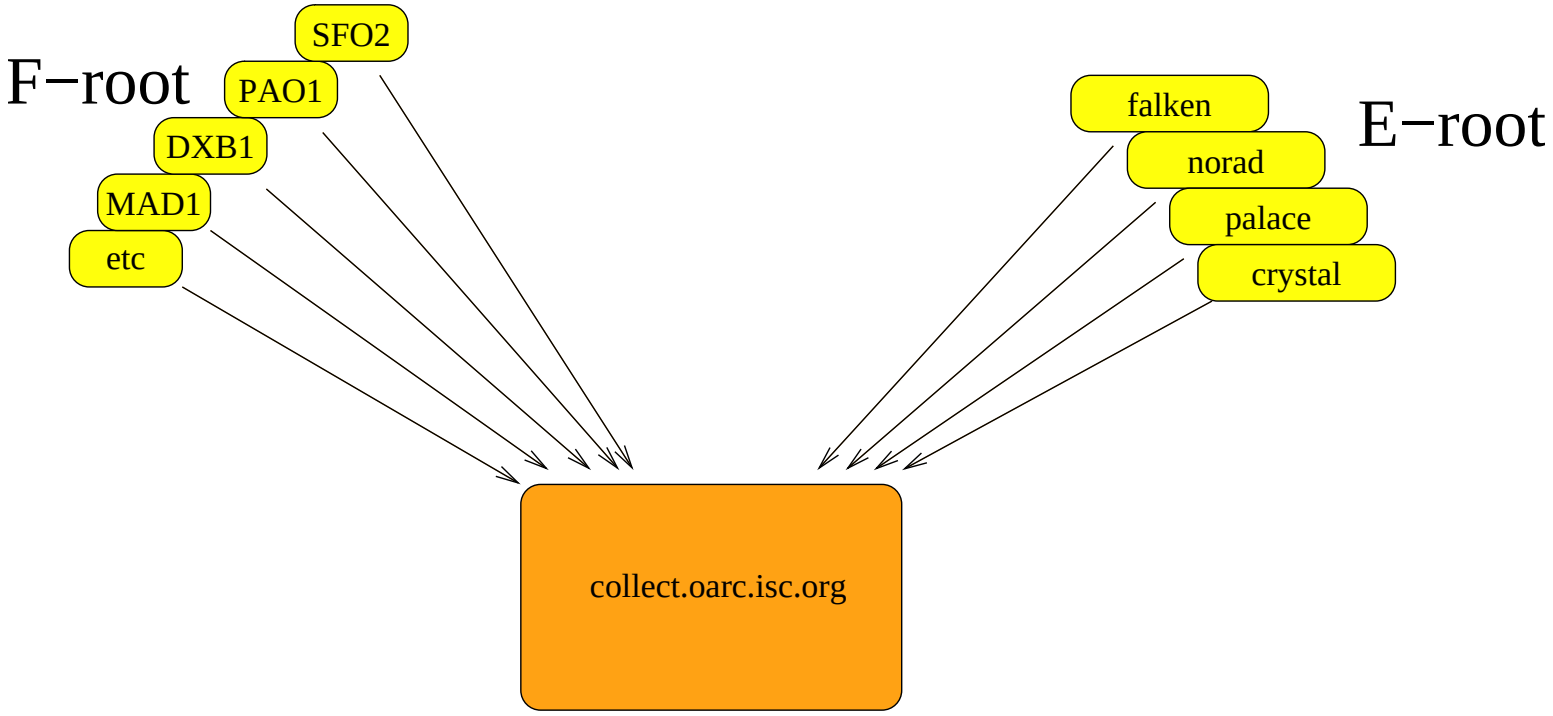
Goals

- Need a coordinated, network-wide view into traffic patterns of critical DNS services.
- Want to collect lots of interesting stats/data on both DNS queries and responses.
- Shipping around full packet capture traces not realistic.
- Use encryption and authentication for security.

Architecture

- A *collector* process runs at or near a DNS server.
- Collector creates a number of 1-D or 2-D "datasets" (histograms) of DNS message characteristics.
- Collector spits out XML-encoded datasets data every minute.
- XML files are securely pushed to central server for viewing and archiving.

Architecture



Pushing Data Around

- Use X.509 server certificates for encryption and authentication.
- Use X.509 client certificates for authentication.
- XML files are tar'd before uploading to reduce SSL session overheads.

Web Interface to Data

- Graphs are generated dynamically.
- Can choose among:
  - Servers (e.g., C-, E-, F-root)
  - Nodes (depends on server)
  - Datasets (many)
  - Axis options (counts, rates, percentages)
- Some graphs have clickable areas (usually the legend) to further explore the data.

A Demo

Problems with the DSC software

- A little too complex
- Can't just `make install`.
- Uses quite a few Perl modules.
- X.509 certificates suck. (You can use *rsync* instead.)
- XML parser uses a lot of CPU.
- A little too BSD-specific
- _____
- _____

Operational Issues

- Not "real time" enough for some operators.
- Too "real time" for others.
- May violate privacy restrictions of some operators.
- At least one operator said they could not allow a collector on their server to communicate directly with the OARC server. Need an intermediary?
- Want different access policies for different users.

Missing Features

- Message processing currently stateless. i.e., cannot count repeated queries or match queries to replies.
- No TCP support.
- UDP fragments ignored.
- SQL Database storage.
- _____
- _____
- _____

The End