

RPKIviz Summary

PARSONS, Inc.

16 August 2016

1 Resource PKI (RPKI) Cache Browser/Visualizer

RPKIviz is a tool intended for any resource holder, which will display the authorization relationships represented in the global RPKI objects and the status of those relationships, for use in diagnosis of RPKI content. This tool is intended to give the user a view of the content of the hierarchy of RPKI objects. RPKIviz provides a web interface for searching and browsing the RPKI cache.

1.1 Data Sources

The tool utilizes the following sources of information:

- Global RPKI RP validator output (e.g. rcynic)
 - resource certificates
 - manifests
 - ROAs
 - Ghostbuster records
- Trust anchors

1.2 Resource Search

The tool allows a user to search for a network resource and be presented a list of matching objects in the global RPKI. The user can then click on a specific object (certificate, ROA, etc) to be presented with a detailed view.

1.3 Resource Certificate View

When viewing a specific resource certificate, the user is presented with the following information:

- RFC3779 resources included in the certificate
- Associated Ghostbuster objects
- Associated ROA objects

- validity period
- Link to parent/grandparent resource certificates
- Links to child resource certificates, if any

Figure 1 shows the RPKIviz display of a portion of the RPKI certificate hierarchy that resulted from a search entered into the search field.

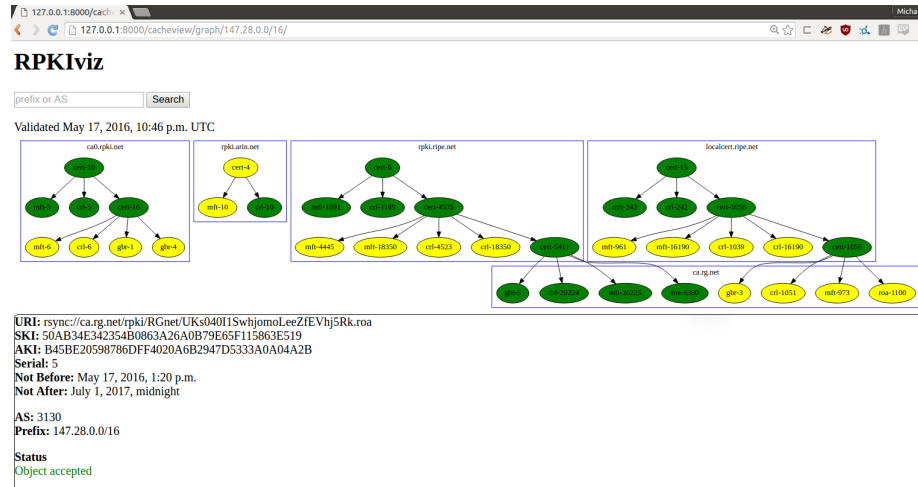


Figure 1: RPKI Tree

1.4 Errors

The RPKIviz tool depicts errors it finds in the RPKI certificates and objects that it displays.

RPKIviz shows Certificates and RPKI objects that have errors in red. Figure fig.error shows several certificates that have errors. It displays the details of one ROA object that has errors and describes the error condition.

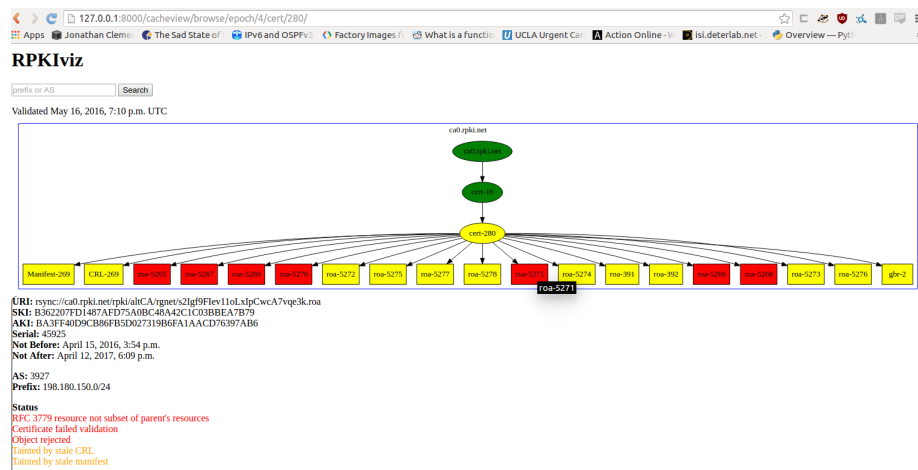


Figure 2: Certificates in Error

1.5 Warnings

The RPKIviz tool will warn if an error condition is looming for an RPKI objects. In particular, it warns if an object is nearing its expiration date.

Figure 3 depicts two certificates in orange, indicating a warning for those certificates.

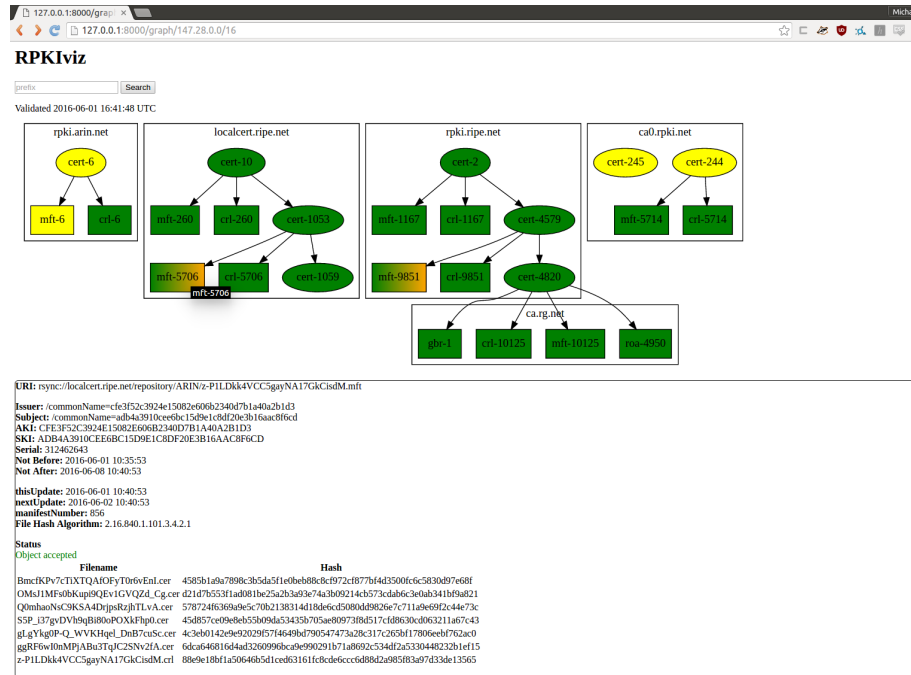


Figure 3: Warning of Impending Error

1.6 History

Portions of the global RPKI repository may be *pruned* when objects expire. Keeping history on objects that used to exist is critical to aid in diagnosis. Otherwise, if a user attempts to use the tool after a grandparent object has expired, it would not necessarily be possible to trace up the tree to determine a cause for grandchild objects disappearing from the global RPKI.

History would also be useful in cases of transfer, so that it would be possible to look back in time to see the resource holders from which a certain resource was transferred.

The RPKIviz tool loads the output of a RPKI relying party validator into a database, so that the history of an object can be displayed. The tool runs the rpki.net RPKI synchronization tool (rcynic) to fetch the RPKI data from the global repositories. It validates the RPKI data, then imports the data into the database.

Figure 4 depicts the history of an RPKI object.

192.169.0.0/23 History

2016-05-10 23:59:38 to 2016-05-11 19:21:06

When	Status	ROAs	Certs
2016-05-10 23:59:38	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 01:15:54	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 04:43:39	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 13:54:45	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 14:21:03	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 15:21:24	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 16:21:21	covered	AS3970	BA3FF... 621A0... A6B69...
2016-05-11 17:44:13	covered	AS3970	BA3FF... 13D4F... 621A0... A6B69...
2016-05-11 18:22:29	covered	AS3970	BA3FF... 13D4F... 621A0... A6B69...
2016-05-11 18:30:42	covered	AS3970	BA3FF... 13D4F... 621A0... A6B69...
2016-05-11 19:21:06	covered	AS3970	BA3FF... 13D4F... 621A0... A6B69...

Figure 4: History

1.7 Trust Anchors

Upon starting, the tool will display a page listing the RIR RPKI Trust Anchors retrieved from the Trust Anchor Locators (TAL) that are distributed with this software.

The ARIN TAL is not distributed with this software. If you wish to use it, you can fetch it from <https://www.arin.net/resources/rpki/tal.html> and include it in the configured set of trust anchors.

There are situations where the users may use a different trust anchor than the RIR trust anchors, for local policy or testing. These can be added to the configured set as well.

Figure 1 shows multiple trust anchors. This particular portion of the RPKI tree shows a prefix that was at the time in the process of transferring from ARIN to RIPE. The figures shows that it was also certified by a local trust anchor.