ROA Expiry

ROA Expiry

This alarm alerts you before the expiration date of a Route Origin Authorization (ROA) record. An ROA record is created by an operator claiming ownership of the resource (advertised prefix) and distributed cryptographically by Regional Internets Registries (RIRs) or other services such as the Routing Assets Database (RADb). For more information, see ripe.net.

You can specify then number of days to be alerted in advance of the ROA record expiring. This is an informational alarm. You can take actions to create a new record to avoid possible filtering of their prefixes by routers. This alarm activates if the prefix is covered by any ROA records and the prefix will not have a valid ROA record at any given time between now and the configured trigger interval (now + **Days to Trigger Before Expiration**). In particular, the alarm does not activate if there is a mix of expired and unexpired records, as long as every point in time in the configured interval has some unexpired covering record.

Possible Problem Detected

This alarm detects a pending lack of ROA coverage.

Relevant Alarm Rule Configurations

The following option must be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > ROA Expiry**):

- Days to trigger before the expiration of an ROA record.

Example

You create a Prefix policy with the **ROA Expiry** alarm rule and linked to prefix 8.8.0.0/24 with 30 **Days to Trigger Before Expiration**. The alarm triggers if prefix 8.8.0.0/24 is covered by multiple ROA records and Crosswork Cloud Network Insights detects that all of these records have already expired or will expire in less than 30 days. To clear the alarm, you should create at least one ROA record for 8.8.0.0/24 covering the trigger time interval.

ROA Expiry