

Operational Monitoring of RPKI Repositories' Health and Safety

<draft-fu-sidrops-rpki-repositories-monitoring-01>

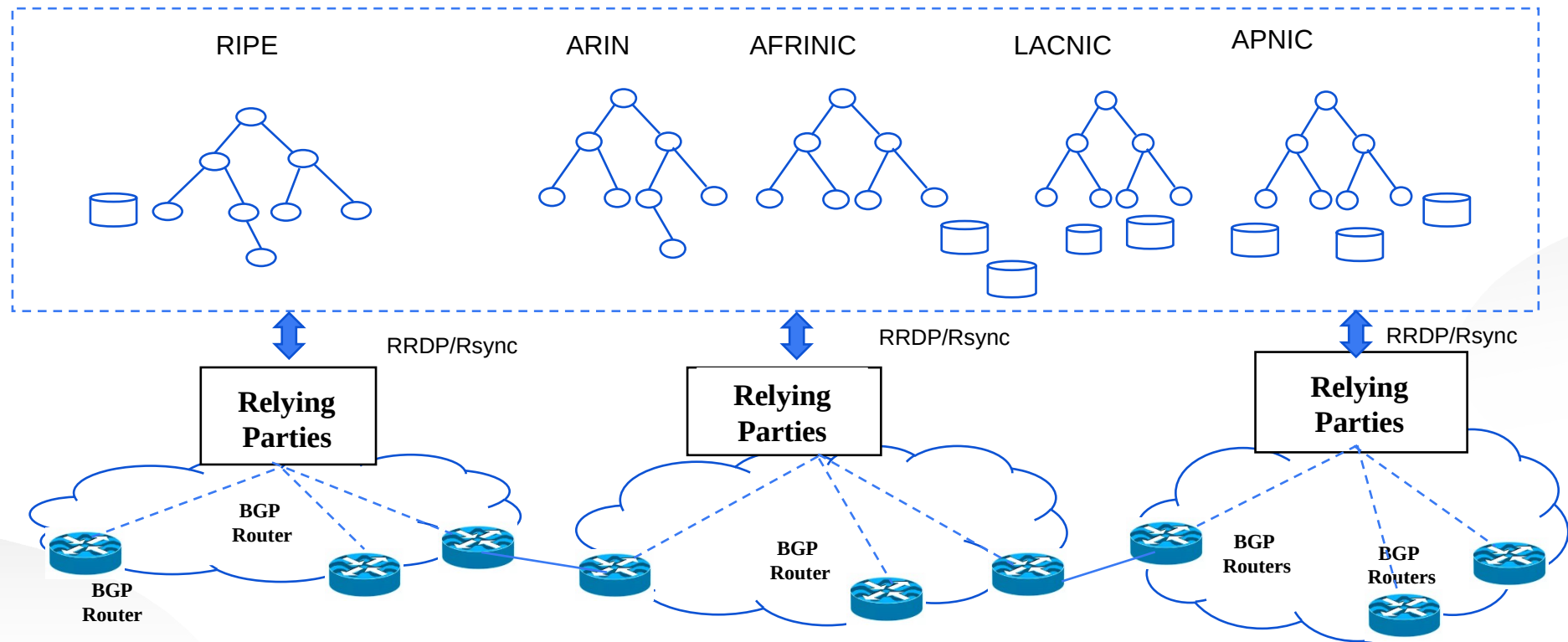
Yonghong Fu, Mingwei Xu, Yangyang Wang, Jia Zhang, Yuanyuan Zhang

IETF 126, July 2026

1 Introduction

The Resource Public Key Infrastructure (RPKI) relies on a globally distributed set of repositories to deliver signed routing authorization data to Relying Parties (RPs).

Global
Distributed
repository
system



2 Problem

In the current RPKI architecture, Relying Parties (RPs) periodically synchronize repository data from the five Regional Internet Registries (RIRs) and distributed Publication Points (PPs). Most existing RP implementations treat synchronization as a global data retrieval process and output only an Validated ROA Payload (VRP) set.

As a result, existing RPKI monitoring approaches providing limited visibility into individual PP behavior and creating operational blind spots for identifying the source of unexpected repository changes or diagnose potential repository issues.

2 Problem

Without per-Publication Point (per-PP) monitoring, an ISP cannot determine whether an unexpected repository state change is caused by a global repository synchronization issue or by a localized failure affecting a specific delegated RPKI repository.

Per-PP monitoring eliminates this ambiguity by providing visibility into each publication point independently. This enables ISPs to accurately pinpoint the source of repository changes, distinguish legitimate updates from abnormal publication point behavior—including operational failures, misconfigurations, and potential malicious activities—and significantly reduce the time required for root cause analysis.

3 Proposal

This draft provides guidance for monitoring the health and safety of RPKI repositories on a per-publicaiton point basis.

It identifies three kinds of indications.

It describes how these indicators can be used to detect degraded or unsafe publication point behavior.

3 Metric Model

Metrics are divided into three classes:

Base Counters:

Primitive observable events. Used for diagnostics and as inputs to derived metrics.

Health Indicators:

Ratios or computed values representing instantaneous repository correctness and usability.

State-Change (Churn) Indicators:

These indicators detect abnormal or unexpected publication behavior over time.

Above metrics are based on per-PP level.

Base Counters

- **DNS Resolution Counters :** Counts of DNS resolution attempts and successful number.
- **Transport Counters:** Counts of TCP/TLS connection attempts and successfully number.
- **Synchronization Counters:** Counts of PP synchronization attempts and the number of synchronization operations successfully completed.
- **Object Retrieval Counters:** Counts of PP objects (e.g., ROAs, CA certificates, manifests, CRLs, etc.) successfully retrieved and the number of object retrievals that failed.
- **Validation Counters:** Counts of repository objects that successfully passed validation and the number of objects that failed validation.

Health Indicators

- **Reachability Indicators:** it measures DNS resolution successful ratio, and the publication point can be contacted ratio.
- **Availability Indicators:** it measures the Fetch Success Ratio, Synchronization Success Ratio, etc.
- **Content Integrity Indicators,** it measures Valid Objects Success Ratio, Object Consistency Ratio (OCR), Hash Mismatch Ratio, etc.

State-Change and Churn Indicators

- **Object Change Count and ratio:** it measures the how many objects are added, removed, or modified, and the corresponding ratio.
- **ROA Stability Indicators:** it measures the how many ROAs are changed, if there are accidental withdrawal or bulk.
- **Certificate and CA Stability Indicators:** it measures the number certificates change, big change maybe key rollover, mass reissuance, misconfiguration, or abnormal behavior.
- **RRDP Publication Continuity indicators:** it measures the srial number of RRDP transfer.

What we can benefit from above metrics

From the fine-grained metrics, operations can have more insight about publication points and diagnose potential issues.

For example, the PPs listed below have all failed to synchronize, but the reasons for their failures are different.

URI	DNS Resolution	TCP/TLS Connection	RRDP
https://krill.ca-bc-01.ssmidge.xyz/rrdp/notification.xml	Success	Fail	Fail
https://feo.tla.org/rrdp/notification.xml	Success	Fail	Fail
https://krill.immarket.space/rrdp/notification.xml	Fail	Fail	Fail
https://krill.signalx.cloud/rrdp/notification.xml	Fail	Fail	Fail
https://orca.rg.net/rrdp/notification.xml	Success	Success	Fail

What we can benefit from above metrics

From the State-Change and Churn Indicators, we can find if a PP has abnormal or unsafe publication behavior. Examples include: sudden bulk withdrawal of ROAs, excessive object churn, incomplete or partially applied updates. Such events can materially affect routing outcomes even when health indicators remain nominal.

7 Conclusion and Next Step Work

This draft provides guidance for monitoring the health and safety of RPKI repositories on a per-publication-point (PP) basis. It defines three categories of metrics: base counters, health indicators, and state-change indicators, which can be used to detect degraded, abnormal, or potentially unsafe repository behavior. Through the proposed monitoring approach, we aim to provide ISPs and RPKI users with greater visibility into the operational status of publication points, helping improve the overall health, reliability, and security of the RPKI ecosystem.

7 Conclusion and Next Step Work

We have deployed multiple Relying Parties (RPs) distributed across different regions worldwide to collect and analyze repository data. In the next phase of our work, we will continue monitoring the proposed metrics, conduct long-term analysis, and validate their effectiveness in identifying repository health issues and security risks. Based on the observations and results, we will further refine the metrics and monitoring methodology to enhance the robustness and practical applicability of RPKI publication-point monitoring.

Q&A
Thanks!