

# A Few Months In The Life Of An RPKI Validator

Rob Austein <[sra@hactrn.net](mailto:sra@hactrn.net)>

Randy Bush <[randy@psg.com](mailto:randy@psg.com)>

Michael Elkins <[Michael.Elkins@sparta.com](mailto:Michael.Elkins@sparta.com)>

... and a lot of help from our friends

IETF 83  
Paris  
March 2012

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# The World As Seen By One RPKI Validator

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>

- ▶ Data as logged by one validator in Seattle.
- ▶ Data collection started late October 2011.
- ▶ Guilty parties are good people, all friends here.
- ▶ Expect updated report(s) at later date(s).

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# A Brief Overview of RPKI Validation

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>

- ▶ Distributed global database of X.509 certificates and dependent objects.
- ▶ The X.509 certificates contain `rsync://` URIs.
- ▶ Validation starts at trust anchor(s).
- ▶ Validator walks certificate tree, following URIs.
- ▶ rcynic is one such validator.
- ▶ rcynic is session-oriented (cron job).

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

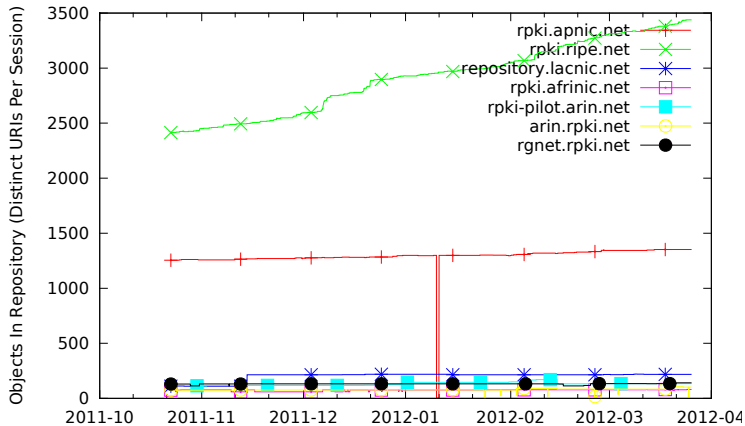
Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Object Counts (Linear)



## Introduction

## Performance Graphs

### Object Counts

### Connection Counts

### Objects/Connection

### Seconds/Object

### Average Connection

### Duration

### Failure Rate

### Rate Limiting

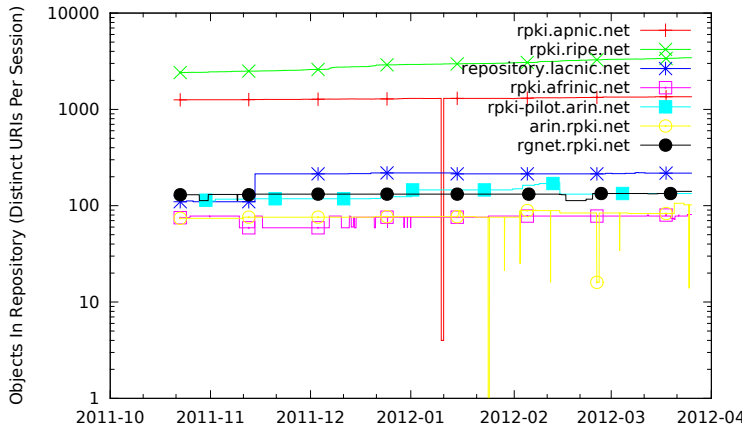
## Repository Summaries

## Conclusion

# Object Counts (Logarithmic)

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>



Introduction

Performance  
Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Average Connection  
Duration
- Failure Rate
- Rate Limiting

Repository  
Summaries

Conclusion

# Object Counts: Observations

- ▶ Large downward spikes are either genuine mass extinction events or, more likely, validation failure of a high-level certificate causing a large subtree to go invalid. Either way, these usually indicate Something Very Bad.

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

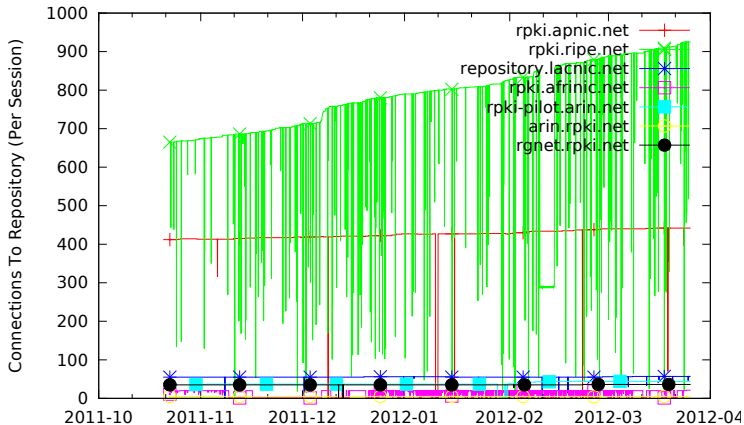
Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Connection Counts (Linear)



## Introduction

## Performance Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Average Connection Duration
- Failure Rate
- Rate Limiting

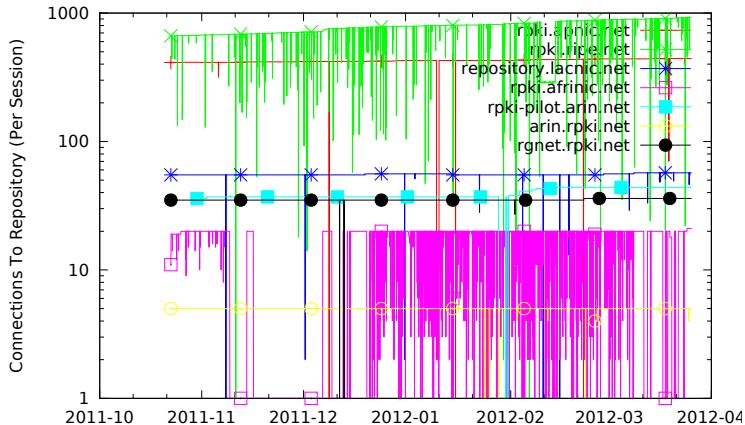
## Repository Summaries

## Conclusion

# Connection Counts (Logarithmic)

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>



Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection

Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion



# Connection Counts: Observations

- ▶ Downward spikes are connection failures, because once we decide a repository server is down, we give up on it until the next session.
- ▶ Are those repositories really that flaky? Perhaps, but at least one of them does their own monitoring and says not. Problem only seems to occur for repositories with AAAA RRs. Uh oh. As far as we can tell this is an IPv6 problem: IPv6 from Seattle to Amsterdam appears to be much flakier than IPv4 from Seattle to Brisbane.

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

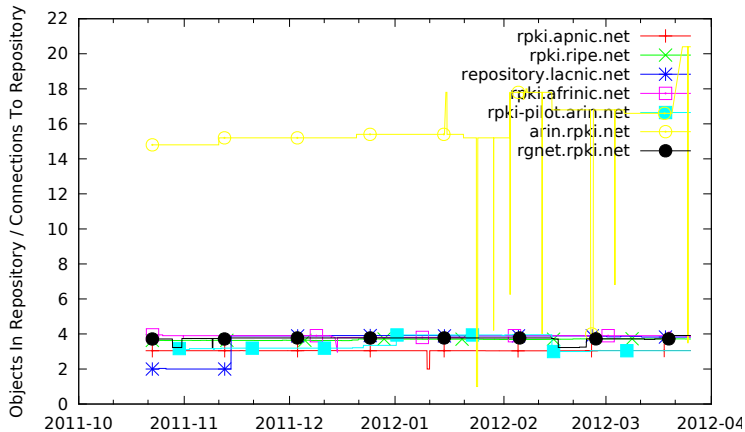
Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Objects/Connection (Linear)



(Sessions with connection failures not shown)

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection

Duration

Failure Rate

Rate Limiting

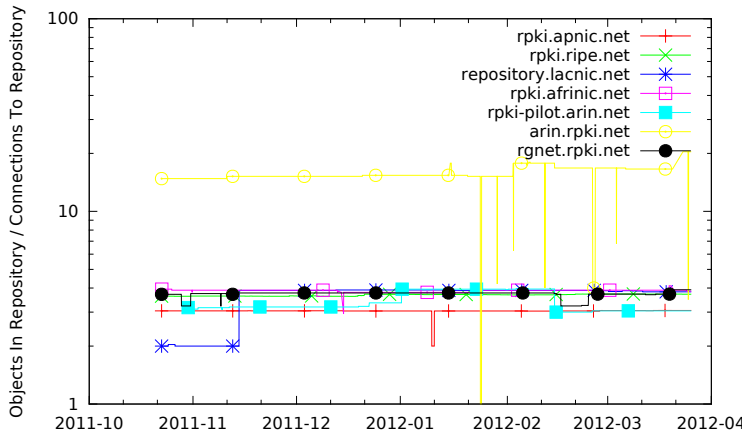
Repository  
Summaries

Conclusion

# Objects/Connection (Logarithmic)

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>



(Sessions with connection failures not shown)

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection

Duration

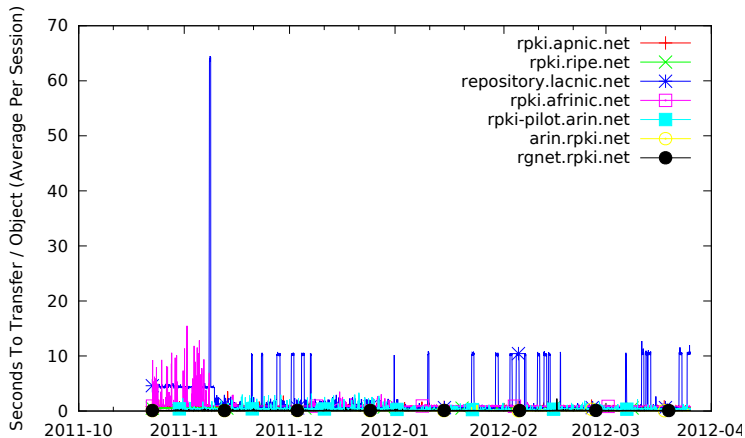
Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Seconds/Object (Linear)



(Sessions with connection failures not shown)

Introduction

Performance  
Graphs

Object Counts  
Connection Counts  
Objects/Connection  
Seconds/Object  
Average Connection  
Duration  
Failure Rate  
Rate Limiting

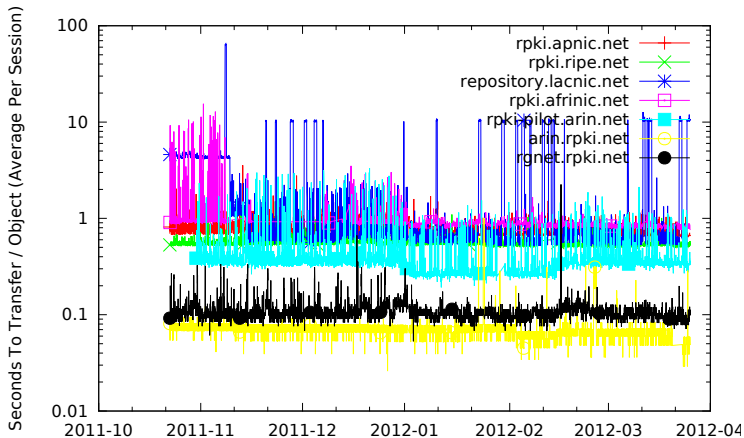
Repository  
Summaries

Conclusion

# Seconds/Object (Logarithmic)

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>



(Sessions with connection failures not shown)

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection

Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Seconds/Object: Observations

- ▶ “Elapsed time” is sum of parallel connection times—five parallel connections of four minutes each counts as twenty minutes.
- ▶ We can speed up in terms of wall time by running more connections in parallel, but that puts more load on the repository servers and risks rate limiting (more on this later).
- ▶ Spikes here are slow repository servers; whether it's the network path or the server itself that's slow, we don't know.

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

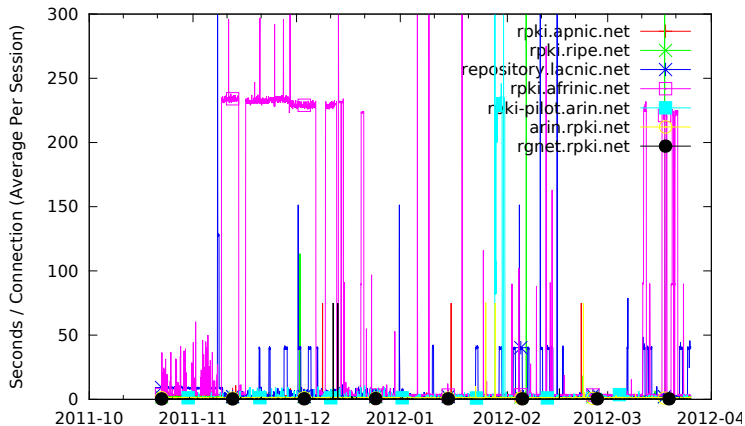
Repository  
Summaries

Conclusion

# Average Connection Duration (Linear)

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>



Introduction

Performance  
Graphs

Object Counts  
Connection Counts  
Objects/Connection  
Seconds/Object

Average Connection  
Duration

Failure Rate  
Rate Limiting

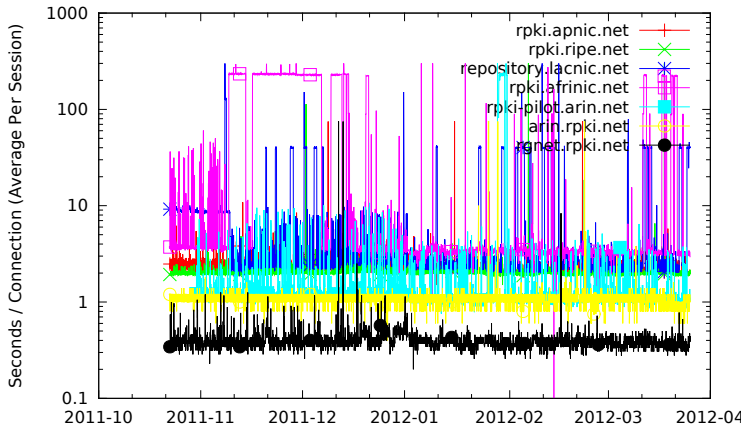
Repository  
Summaries

Conclusion

# Average Connection Duration (Logarithmic)

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>



Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion



# Average Connection Duration: Observations

- ▶ Early modeling and testing said much of cost is setup and teardown (about 500ms) and that this cost tends to dominate for large numbers of connections. So far, this analysis has held up pretty well.
- ▶ Spikes top out at 300 seconds because that's when rcynic gives up and whacks any rsync subprocess that appears to be completely stalled. This shouldn't happen, and generally indicates that repository server or network is badly messed up.

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

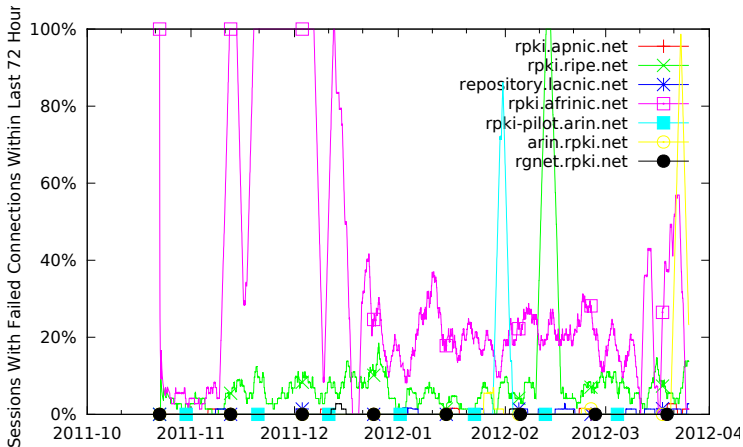
Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Failure Rate (Linear)



## Introduction

## Performance Graphs

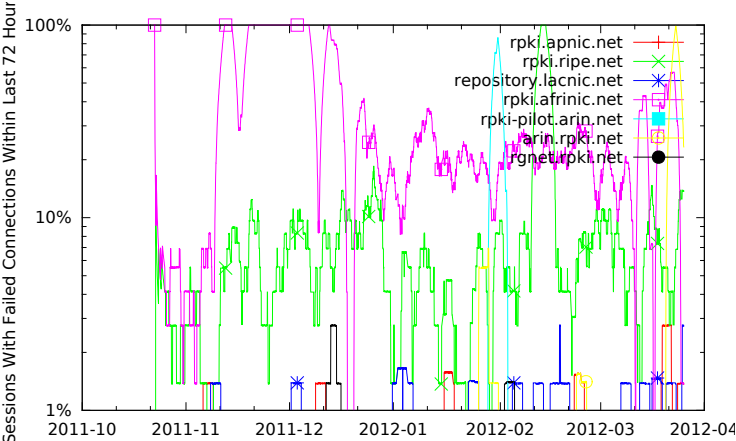
- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Average Connection Duration

- Failure Rate
- Rate Limiting

## Repository Summaries

## Conclusion

# Failure Rate (Logarithmic)



Introduction

Performance  
Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Average Connection Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Failure Rate: Observations

- ▶ Failure rate is a bit hard to measure because:
  - ▶ We give up on a repository host for the duration of that session after the first failure.
  - ▶ rsync exit codes often don't tell us much we can use.
- ▶ For example, a valid certificate containing an incorrect SIA URI can result in a failure attempting to fetch from the named repository, with rsync exit code #23, "Partial transfer due to error."
- ▶ So shape of the curve is significant: a brief spike from 0% to 100% is probably a data error rather than a network issue, while a failure rate that wanders all over the map is probably a network or server.

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Rate Limiting (Sorry, No Graph)

- ▶ APNIC and AfrinIC used to rate limit to four connections in rsyncd.conf. Both appear to have stopped doing this.
- ▶ At one point APNIC also appeared to be rate limiting with some kind of firewall . . . which is harder to adapt to than rsyncd.conf limit. Haven't seen evidence of this recently.
- ▶ Others repositories currently appear to impose no rate limits.
- ▶ Rate limiting is a hard problem. What's the right limit for how many parallel rsync connections a validator should try? How should repository operator push back when overloaded?

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Sample Of Rcynic Status Output

- ▶ The following are samples of rcynic's normal output for the repositories in question.
- ▶ Some things are easier to see in this form, some are easier to see as graphs.
- ▶ We're still experimenting with how best to present these data.

# Summary for rpki.apnic.net 2012-03-26T06:10:44Z

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	RFC 3779 resource not subset of parent's resources	AKI extension issuer mismatch	Bad keyUsage	Certificate failed validation	CRLDP doesn't match issuer's SIA	Manifest list missing object	Object rejected	ryse transfer failed	AAA doesn't match issuer	EE certificate with 1024 bit key	Multiple ryse URLs in extension	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	State CRL or manifest	Tainted by state CRL	Tainted by state manifest	Tainted by not being in manifest	Unknown object type skipped	Non-ryse URL in extension	Object accepted	ryse transfer succeeded
																						442	
carum cst														442	1							442	
carum crl														1								442	
carum cst0														1								442	
carum cst1																						26	
Total											17	17		442	1							1382	442

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Summary for rpki.ripe.net 2012-03-26T06:10:44Z

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	RFC 3779 resource not subset of parent's resources	AKI extension issuer mismatch	Bad keyUsage	Certificate failed validation	CRLDP doesn't match issuer's SIA	Manifest bits missing object	Object rejected	sync transfer failed	AAA doesn't match issuer	EE certificate with 1024 bit key	Multiple cync ERIs in extension	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	State CRL or manifest	Tainted by state CRL	Tainted by state manifest	Tainted by not being in manifest	Unknown object type skipped	Non-csync ERI in extension	Object accepted	sync transfer succeeded
																						925	
carum.cir														922	101							924	
carum.crl														101								924	
carum.inf														101	1							924	
backup.rta										2								2				2	
carum.rta										670				175	67							666	
Total										681				1299	119			2				3440	925

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion



# Summary for repository.lacnic.net 2012-03-26T06:10:44Z

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	RFC 3779 resource not subset of parent's resources	AKI extension issuer mismatch	Bad keyUsage	Certificate failed validation	CRLDP doesn't match issuer's SIA	Manifest list missing object	Object rejected	ryse transfer failed	AAA doesn't match issuer	EE certificate with 1024 bit key	Multiple ryse URLs in extension	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	State CRL or manifest	Tainted by state CRL	Tainted by state manifest	Tainted by not being in manifest	Unknown object type skipped	Non-ryse URL in extension	Object accepted	ryse transfer succeeded
																						57	
carum cst														2	1							56	
carum crl														1								56	
carum cst0														1								56	
carum cst1														1								50	
Total														4	1							216	57

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Summary for rpki.afrinic.net 2012-03-26T06:10:44Z

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	RFC 3779 resource not subset of parent's resources	AKI extension issuer mismatch	Bad keyUsage	Certificate failed validation	CRLDP doesn't match issuer's SIA	Manifest list missing object	Object rejected	rysmc transfer failed	AAA doesn't match issuer	EE certificate with 1024 bit key	Multiple rysmc URLs in extension	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	State CRL or manifest	Tainted by state CRL	Tainted by state manifest	Tainted by not being in manifest	Unknown object type skipped	Non-rysmc URL in extension	Object accepted	rysmc transfer succeeded
																				2		20	
carrou cot																				1	20		
carrou crl																					20		
carrou crl0											1										1	20	
carrou crl1																						21	
Total											1									2	2	61	21

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Summary for rpki-pilot.arin.net 2012-03-26T06:10:44Z

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	RFC 3779 resource not subset of parent's resources	AKI extension issuer mismatch	Bad keyUsage	Certificate failed validation	CRLDP doesn't match issuer's SIA	Manifest line missing object	Object rejected	rync transfer failed	AAA doesn't match issuer	EE certificate with 1024 bit key	Multiple rync URLs in extension	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	State CRL or manifest	Tainted by state CRL	Tainted by state manifest	Tainted by not being in manifest	Unknown object type skipped	Non-rync URL in extension	Object accepted	rync transfer succeeded
																						66	66
cares cert															37		43		44			44	
cares crl																2						2	
cares leaf														37	14								
cares root															34	36							44
Total										4	4			35	47	2	43		44		46	44	

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Summary for arin.rpki.net 2012-03-26T06:10:44Z

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	RFC 3779 resource not subset of parent's resources	AKI extension issuer mismatch	Bad keyUsage	Certificate failed validation	CRLDP doesn't match issuer's SIA	Manifest line missing object	Object rejected	rsync transfer failed	AAA doesn't match issuer	EE certificate with 1024 bit key	Multiple rsync CRLs in extension	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	State CRL or manifest	Tablated by state CRL	Tablated by state manifest	Tablated by not being in manifest	Unknown object type skipped	Non-rsync URI in extension	Object accepted	rsync transfer succeeded
carum.cer																		1			12	0	
backup.crl																1						1	
carum.crl																1						0	
carum.gbr				0					0		0							0				1	
carum.mfi																1	1					0	
backup.mfi																1	1					1	
backup.rta																	0	3	3			0	
carum.rta	0			0		1		1	12		0						1	12				0	
Total	0			0		1		1	20		0					0	0	6	20		0	0	

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Summary for rgnet.rpki.net 2012-03-26T06:10:44Z

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	RFC 3779 resource not subset of parent's resources	AKI extension issuer mismatch	Bad keyUsage	Certificate failed validation	CRLDP doesn't match issuer's SIA	Manifest list missing object	Object rejected	rync transfer failed	AAA doesn't match issuer	EE certificate with 1024 bit key	Multiple rync URLs in extension	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	State CRL or manifest	Tainted by state CRL	Tainted by state manifest	Tainted by not being in manifest	Unknown object type skipped	Non-rync URL in extension	Object accepted	rync transfer succeeded
																						36	
current crl																						35	
current crl																						36	
current crl	1	1				2			2									2				1	
current crl																						36	
current crl																						29	
Total	1	1				2			2									2				139	36

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Things We're Not Measuring (Yet?)

**Freshness:** Some kind of measure of whether we're keeping up with what's being published, regardless of how we do it or how much pain is involved. One could make a case that this is the critical measurement and that all else is just dickering over the price.

What else?

Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion

# Problems We Think We're Seeing

- ▶ Slow repository servers are an issue for validator, whether they fail or not.
- ▶ Flat repository structure is an issue for validator.
- ▶ Rate limiting is an issue for validator and repository operator.
- ▶ Validator might not need to poll every URI every session.
- ▶ Alternate transports worth investigating (*e.g.* BitTorrent, separate presentation).

# Questions?

A Few Months In  
The Life Of An  
RPKI Validator

<http://rpki.net/>



Introduction

Performance  
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Average Connection  
Duration

Failure Rate

Rate Limiting

Repository  
Summaries

Conclusion