

A Few Weeks In The Life Of An RPKI Validator

Rob Austein <sra@hactrn.net>

Randy Bush <randy@psg.com>

Michael Elkins <Michael.Elkins@cobham.com>

... and a lot of help from our friends

IEPG, Taipei, 13 November 2011

The World As Seen By One RPKI Validator

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>

- ▶ Data as logged by one validator in Seattle
- ▶ Data collection started around 22 October 2011
- ▶ Results are very preliminary
- ▶ Guilty parties are good people, will likely fix
- ▶ Expect updated report at some later date

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

A Brief Overview of RPKI Validation

A Few Weeks 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://` URLs
- ▶ 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

Length of Average
Connection

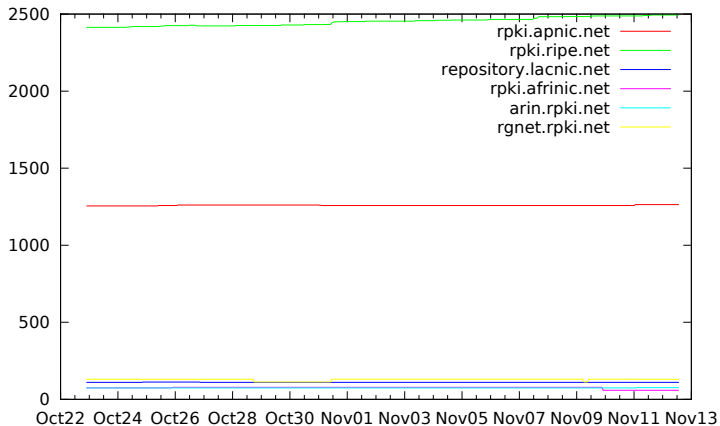
Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Object Counts (Linear)



Introduction

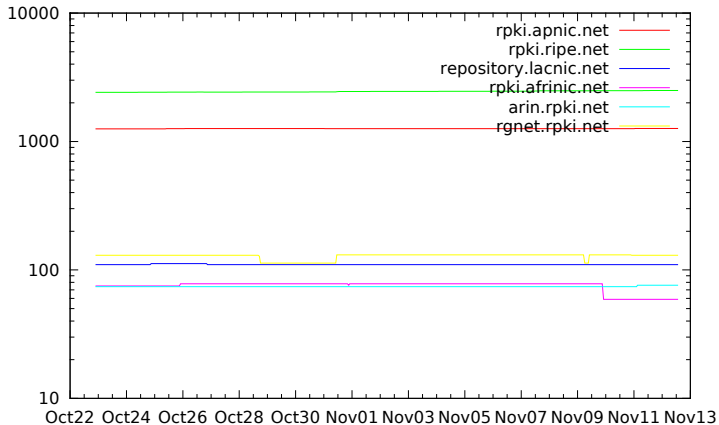
Performance Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Length of Average Connection
- Failure Rate
- Rate Limiting

Repository Summaries

Conclusion

Object Counts (Logarithmic)



Introduction

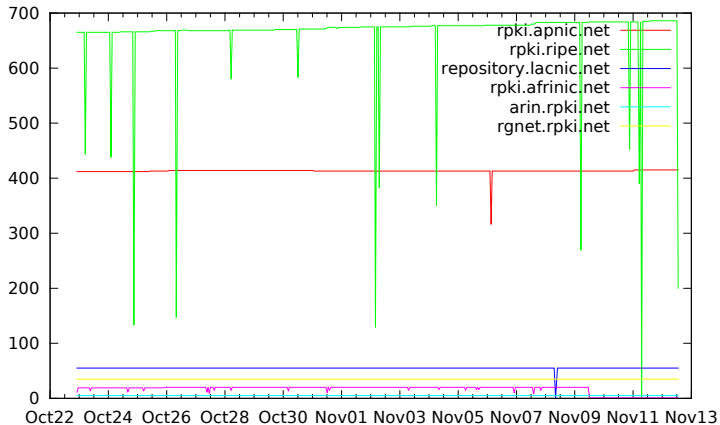
Performance Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Length of Average
Connection
- Failure Rate
- Rate Limiting

Repository Summaries

Conclusion

Connection Counts (Linear)



Introduction

Performance Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Length of Average Connection
- Failure Rate
- Rate Limiting

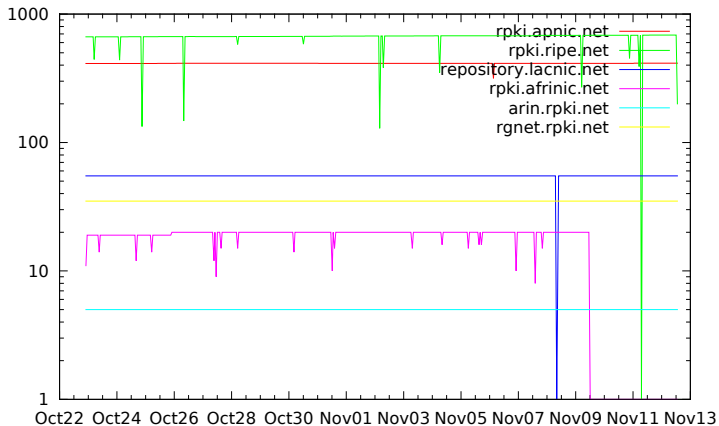
Repository Summaries

Conclusion

Connection Counts (Logarithmic)

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>



Introduction

Performance
Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Length of Average
Connection
- Failure Rate
- Rate Limiting

Repository
Summaries

Conclusion

Connection Counts: Observations

- ▶ Spikes are connection failures
- ▶ APNIC and RIPE require a lot of connections
 - ▶ Partly because they have a lot of objects
 - ▶ But also because they use flat repository structure

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

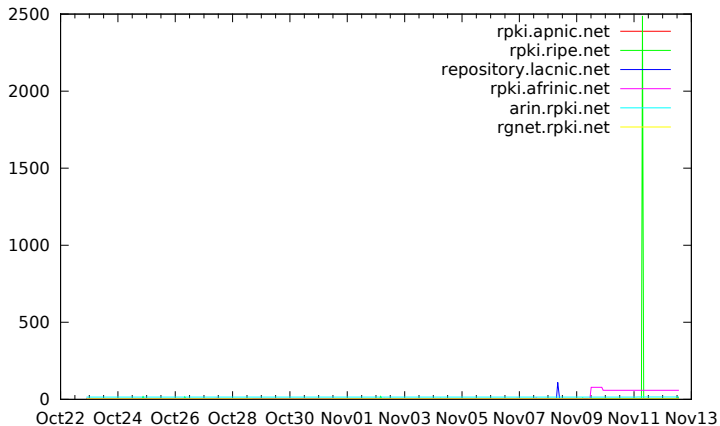
Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Objects/Connection (Linear)



Introduction

Performance Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Length of Average Connection
- Failure Rate
- Rate Limiting

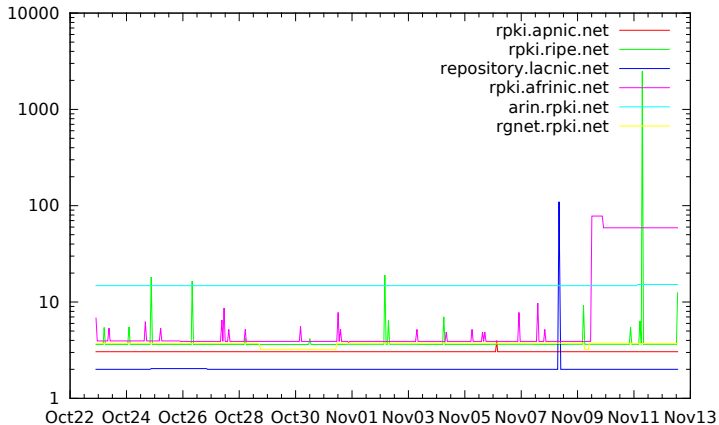
Repository Summaries

Conclusion

Objects/Connection (Logarithmic)

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>



Introduction

Performance
Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Length of Average Connection
- Failure Rate
- Rate Limiting

Repository
Summaries

Conclusion

Objects/Connection: Observations

- ▶ Spikes are connection failures
- ▶ Pseudo-ARIN is optimally organized repository
- ▶ RGnet, running same code, is not
- ▶ Something interesting happened at AfriNIC
 - ▶ Started as persistent connection failure
 - ▶ Then manifest expirations dropped object count

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

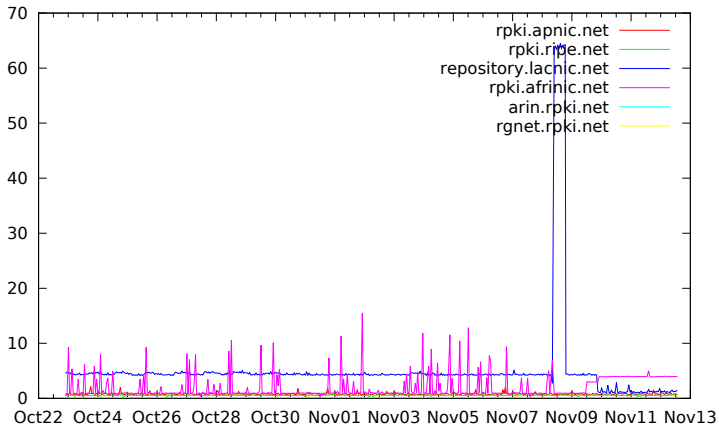
Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Seconds/Object (Linear)



Introduction

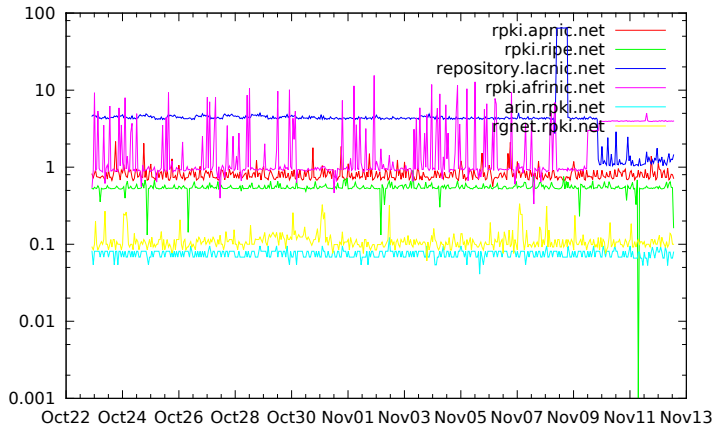
Performance Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Length of Average
Connection
- Failure Rate
- Rate Limiting

Repository Summaries

Conclusion

Seconds/Object (Logarithmic)



Introduction

Performance Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Length of Average Connection
- Failure Rate
- Rate Limiting

Repository Summaries

Conclusion

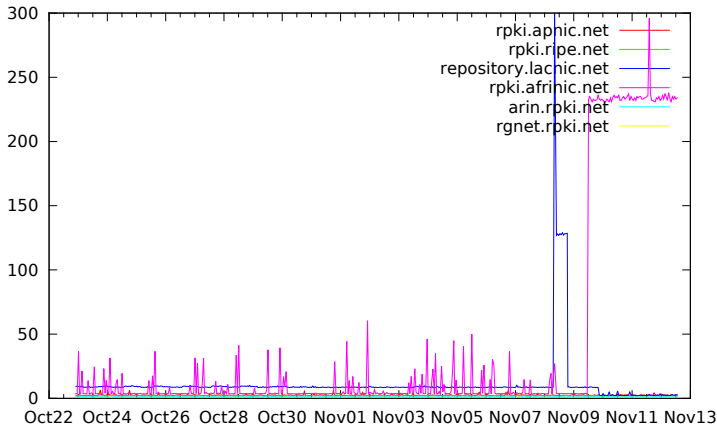
Seconds/Object: Observations

- ▶ “Elapsed time” is sum of parallel connection times
 - ▶ So five parallel connections of four minutes each counts as twenty minutes
- ▶ AfriNIC timing is all over the place, perhaps due to long pipe
- ▶ AfriNIC plateau is some kind of slow connection failure
- ▶ LACNIC is consistently bad, except when it's terrible
- ▶ LACNIC plateau is (presumably unintended) tarpit
- ▶ RIPE and APNIC are pretty fast
- ▶ Optimized repository (Pseudo-ARIN) looks faster than repository in same rack as validator (rgnet), but not enough data to tell whether difference is significant

Length of Average Connection (Linear)

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>



Introduction

Performance
Graphs

Object Counts
Connection Counts
Objects/Connection
Seconds/Object

Length of Average
Connection

Failure Rate
Rate Limiting

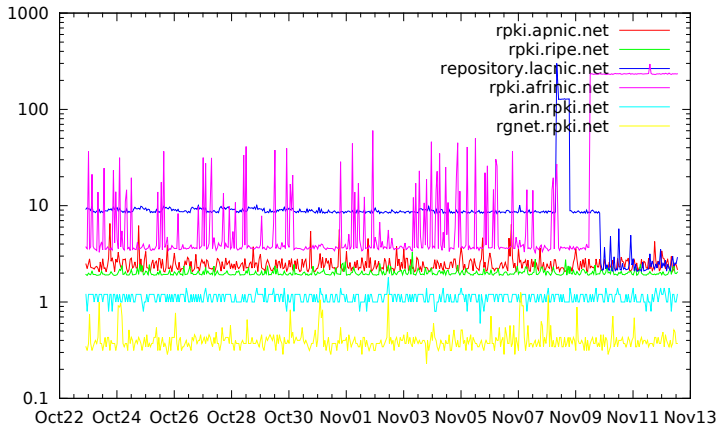
Repository
Summaries

Conclusion

Length Average Connection (Logarithmic)

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>



Introduction

Performance
Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Length of Average
Connection
- Failure Rate
- Rate Limiting

Repository
Summaries

Conclusion

Length Average Connection: Observations

- ▶ AfriNIC is all over the place again
- ▶ LACNIC is kinda slow
- ▶ LACNIC spike is forced termination (bug? tarpit?)
- ▶ APNIC and RIPE are reasonably fast, it's the number of connections that hurts
 - ▶ This is consistent with early modeling and testing
 - ▶ Cost is probably setup and teardown (about 500ms)

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

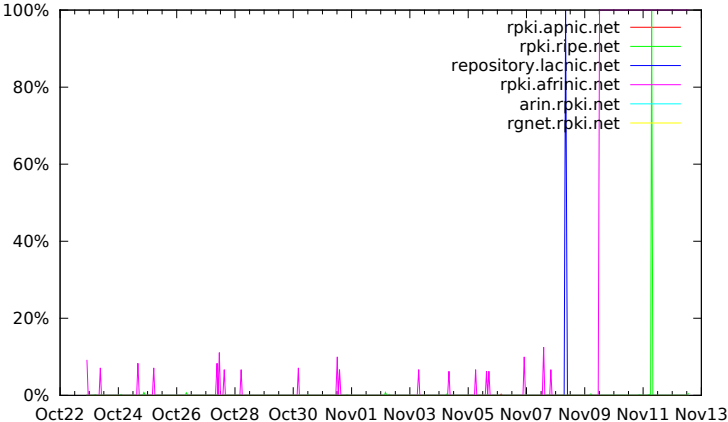
Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Failure Rate (Linear)



Introduction

Performance
Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Length of Average Connection

Failure Rate
Rate Limiting

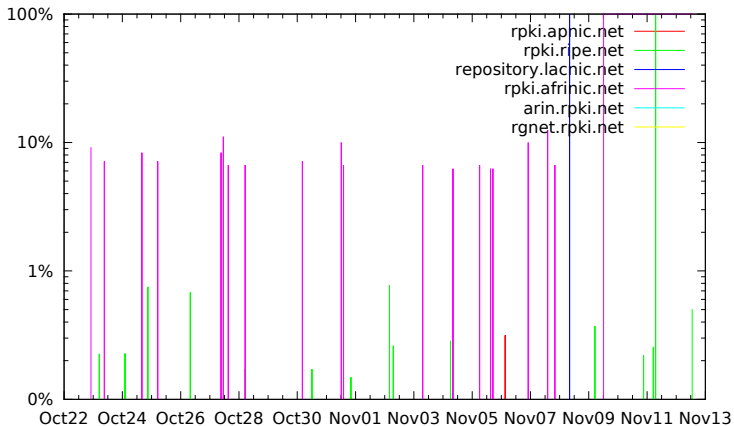
Repository
Summaries

Conclusion

Failure Rate (Logarithmic)

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>



Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average

Connection

Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Failure Rate: Observations

- ▶ Rates are relative to total number of connections
- ▶ One failure per repository per session
- ▶ AfriNIC and LACNIC each had hard outages
- ▶ AfriNIC has relatively high failure rate even when not down

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Rate Limiting (Sorry, No Graph)

- ▶ AfriNIC rate limits to four connections in rsyncd.conf
- ▶ APNIC appears to rate limit with some kind of firewall . . . which is harder to adapt to than rsyncd.conf limit
- ▶ Others currently appear to impose no rate limits
- ▶ This is, potentially, a hard problem

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Sample Of Rcynic Status Output

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>

- ▶ 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 to present these data

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Summary for rpki.apnic.net 2011-11-12T13:07:31Z

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	AIA doesn't match issuer	Certificate failed validation	CRL not yet valid	Manifest not yet valid	Object rejected	rsync transfer failed	Digest mismatch	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Object accepted	rsync transfer succeeded
																	415
current .cer										413	1					415	
current .crl																415	
backup .mft										1							
current .mft									1	1						415	
current .roa																19	
Total									1	415	1					1264	415

Introduction

Performance
Graphs

Object Counts
Connection Counts
Objects/Connection
Seconds/Object
Length of Average
Connection
Failure Rate
Rate Limiting

Repository
Summaries

Conclusion

Summary for rpki.ripe.net 2011-11-12T13:07:31Z

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	AIA doesn't match issuer	Certificate failed validation	CRL not yet valid	Manifest not yet valid	Object rejected	rsync transfer failed	Digest mismatch	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Object accepted	rsync transfer succeeded
								1									199
current .cer										683	101					685	
current .crl																685	
backup .mft										101	1						
current .mft										101	1					685	
current .roa										113	66					439	
Total								1		998	169					2494	199

Introduction

Performance
Graphs

Object Counts
Connection Counts
Objects/Connection
Seconds/Object
Length of Average
Connection
Failure Rate
Rate Limiting

Repository
Summaries

Conclusion

Summary for repository.lacnic.net 2011-11-12T13:07:31Z

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	AIA doesn't match issuer	Certificate failed validation	CRL not yet valid	Manifest not yet valid	Object rejected	rsync transfer failed	Digest mismatch	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Object accepted	rsync transfer succeeded
																	55
current .cer										2	22					54	
current .crl																2	
backup .mft										1	1						
current .mft			52				52			1	1					2	
Total			52				52			4	24					58	55

Introduction

Performance
Graphs

Object Counts
Connection Counts
Objects/Connection
Seconds/Object
Length of Average
Connection
Failure Rate
Rate Limiting

Repository
Summaries

Conclusion

Summary for rpki.afrinic.net 2011-11-12T13:07:31Z

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	AIA doesn't match issuer	Certificate failed validation	CRL not yet valid	Manifest not yet valid	Object rejected	rsync transfer failed	Digest mismatch	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Object accepted	rsync transfer succeeded
								1									
backup .cer													17		17	17	
current .cer																2	
backup .crl												18					
current .crl												18				19	
current .mft	18			18			18						18			1	
backup .roa															19		
current .roa													19			19	
Total	18			18			18	1				36	54		36	58	

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Summary for arin.rpki.net 2011-11-12T13:07:31Z

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>

	certificate has expired	certificate revoked	AIA doesn't match issuer	Certificate failed validation	CRL not yet valid	Manifest not yet valid	Object rejected	rsync transfer failed	Digest mismatch	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Object accepted	rsync transfer succeeded
																	5
current .cer																17	
backup .crl												2					
current .crl												2				9	
backup .mf												2	2				
current .mf												2	2			9	
backup .roa														6			
current .roa													6	6		41	
Total												8	10	12		76	5

Introduction

Performance
Graphs

Object Counts
Connection Counts
Objects/Connection
Seconds/Object
Length of Average
Connection
Failure Rate
Rate Limiting

Repository
Summaries

Conclusion

Summary for rgnet.rpki.net 2011-11-12T13:07:31Z

	certificate has expired	certificate revoked	AIA doesn't match issuer	Certificate failed validation	CRL not yet valid	Manifest not yet valid	Object rejected	rsync transfer failed	Digest mismatch	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Object accepted	rsync transfer succeeded
																	35
current .cer																34	
backup .crl												1					
current .crl																35	
current .gbr																2	
backup .mnf												1					
current .mnf																35	
current .roa																24	
Total												2				130	35

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Summary for rpki.surfnet.nl 2011-11-12T13:07:31Z

	certificate has expired	certificate revoked	AIA doesn't match issuer	Certificate failed validation	CRL not yet valid	Manifest not yet valid	Object rejected	rsync transfer failed	Digest mismatch	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Object accepted	rsync transfer succeeded
																	1
backup.crl												1					
current.crl												1				1	
backup.mnf												1	1				
current.mnf												1	1			1	
Total												4	2			2	1

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Problems We Think We're Seeing

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>

- ▶ Slow 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
- ▶ Validator might not need to poll every URI every session

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Gentlebeings, Start Your Engines

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>

- ▶ Drawing pictures is easy
- ▶ Learning anything useful from them is harder
- ▶ We're still figuring out how to interpret these measurements
- ▶ Now is the time to start debugging and tuning, before we bet operations on this

Introduction

Performance
Graphs

Object Counts

Connection Counts

Objects/Connection

Seconds/Object

Length of Average
Connection

Failure Rate

Rate Limiting

Repository
Summaries

Conclusion

Questions?

A Few Weeks In
The Life Of An
RPKI Validator

<http://rpki.net/>



Introduction

Performance
Graphs

- Object Counts
- Connection Counts
- Objects/Connection
- Seconds/Object
- Length of Average
Connection
- Failure Rate
- Rate Limiting

Repository
Summaries

Conclusion