HAWK-EYE

RIVERBED PERFORMANCE MONITORING

Deep dive

SSL

Created for CUSTOMER

December 17th 2018 - December 31st 2018

| Riverbed Elite Partner | Riverbed Authorized Support Partner | Riverbed Authorized Consulting Partner |
| Riverbed Managed Service Provider |

Contents

Introduction

Preface

This report takes a deep-dive into the SSL protocol optimization on SteelHeads within your estate. The report includes details of the error profiles in your network. It is not the intention of the report to give recommendations or advise on how to troubleshoot or reconfigure the SteelHead estate. The report is meant as a detailed technical health overview of the SSL protocol optimization only. Only known ports where SSL could be used, is taken into consideration. Currently we monitor port 443, 444, 7830 and 944.

SteelHeads in Scope

This shows a list of SteelHeads that have been analyzed.

Total number of monitored devices: 9

Site	Model	RiOS version
Steelhead-01	CX5070M	9.7.1
Steelhead-02	CX570M	9.7.1
Steelhead-03	CX770L	9.7.1
Steelhead-04	250H	9.1.0a
Steelhead-05	CX3070L	9.7.1
Steelhead-06	CX570L	9.7.1
Steelhead-07	CX570M	9.7.1
Steelhead-08	CX570L	9.7.1
Steelhead-09	CX5070M	9.7.1

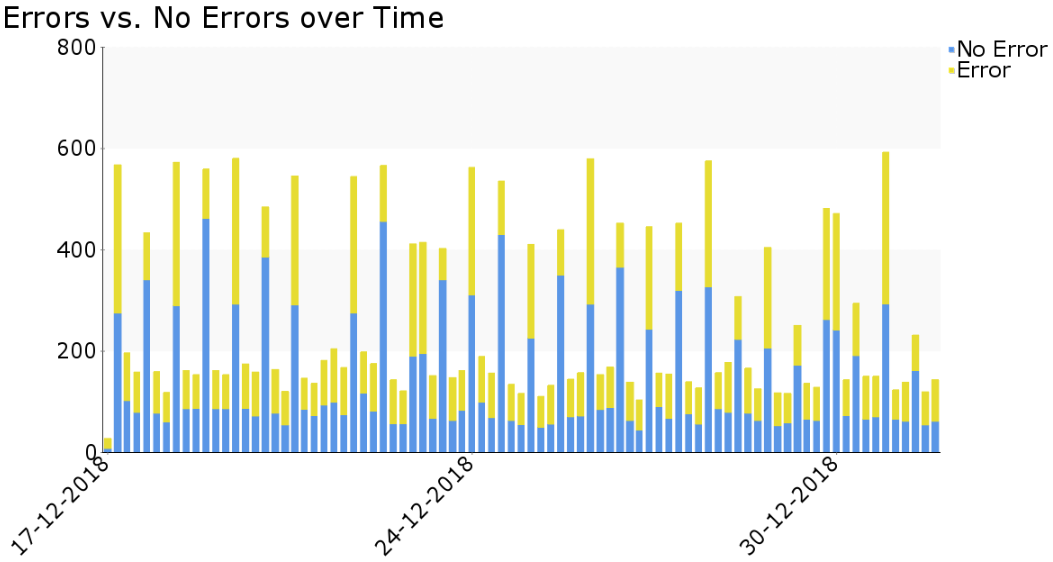
The following sites are excluded from this report

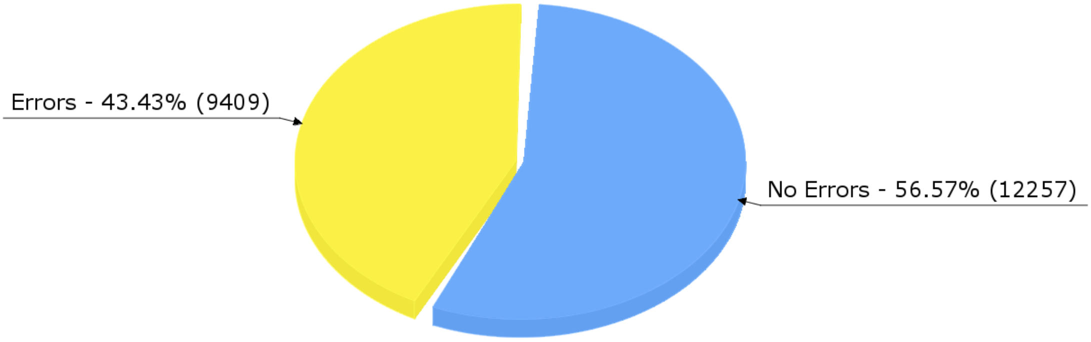
Site	Issue
Steelhead-10	Device implemented November 1st 2018. That means that we are missing 33% data

Optimization Errors vs. No Errors

In this section we have analyzed how many errors were logged, comparing it to the number of sessions optimized with no errors. Please note that an error is not a session that is broken from the user perspective it's an error in the optimization.

When we see optimization errors, it means the SteelHead cannot perform layer7 optimization, but is only capable of bandwidth optimization. Without Layer 7 optimization, users will experience significant performance degradation, in particular this will impact those links and sites with high latency.

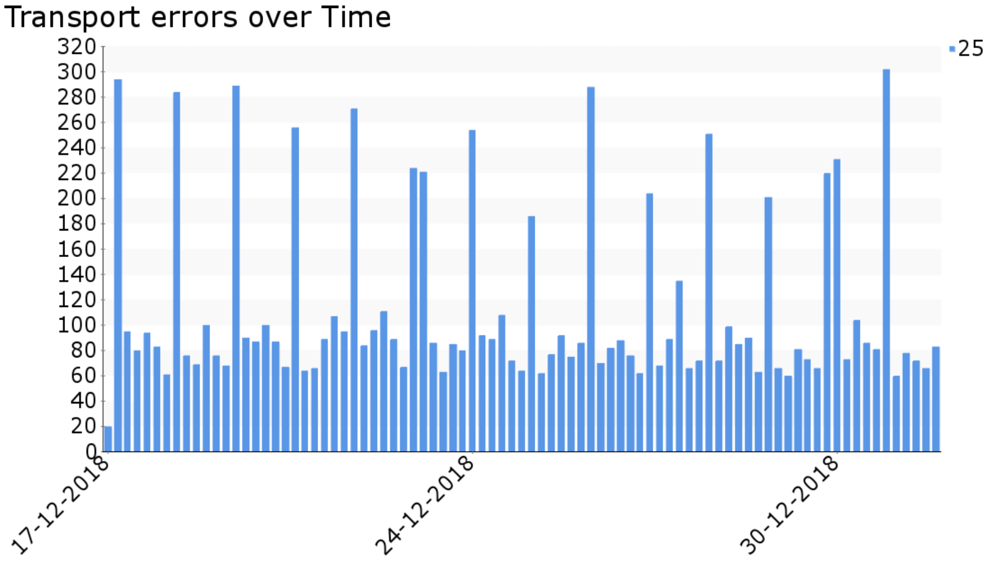


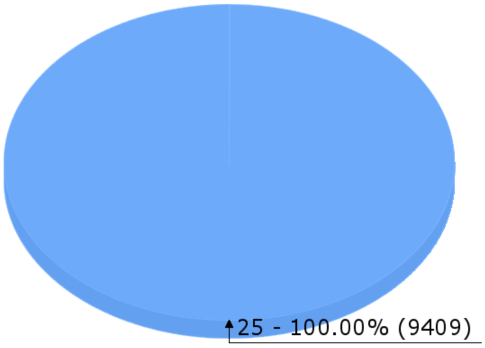


Transport errors

When a transport error occurs, the SteelHead lists a reason why the event occurred. There will be many different causes, but the most common is a failed SSL handshake.
The transport error code list is the official Riverbed one and is available from the Riverbed knowledge base or from the appendix to this report.

This view is global, but in later sections you will be able to see what SteelHeads, servers or clients are causing the errors.

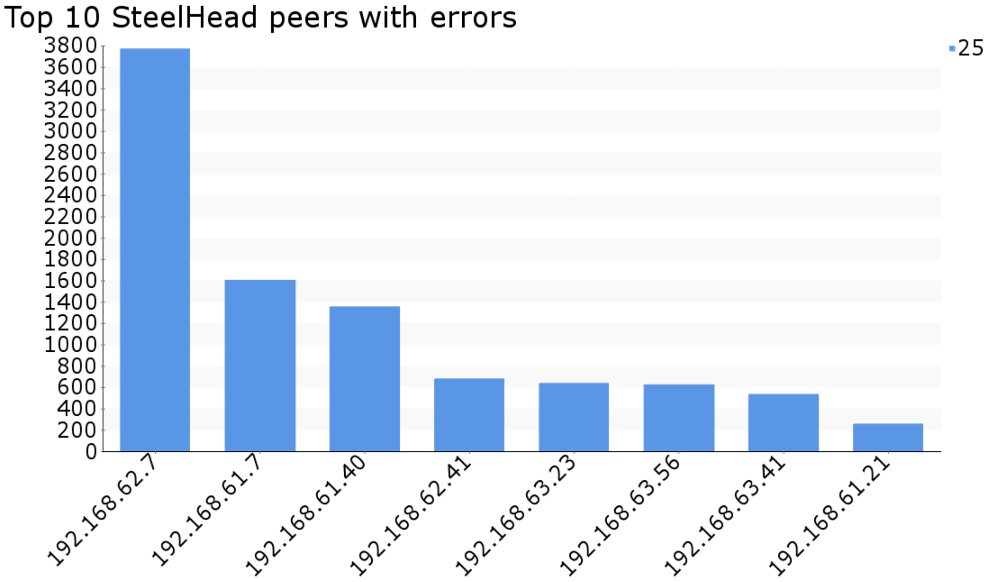




Top 10 SteelHead peers with errors

When we analyze a session, data is collected to identify the server-side SteelHeads. We use this information to detect SteelHeads that have problems, helping you to identify and prioritize the SteelHeads that needs to be focused on when troubleshooting issues.

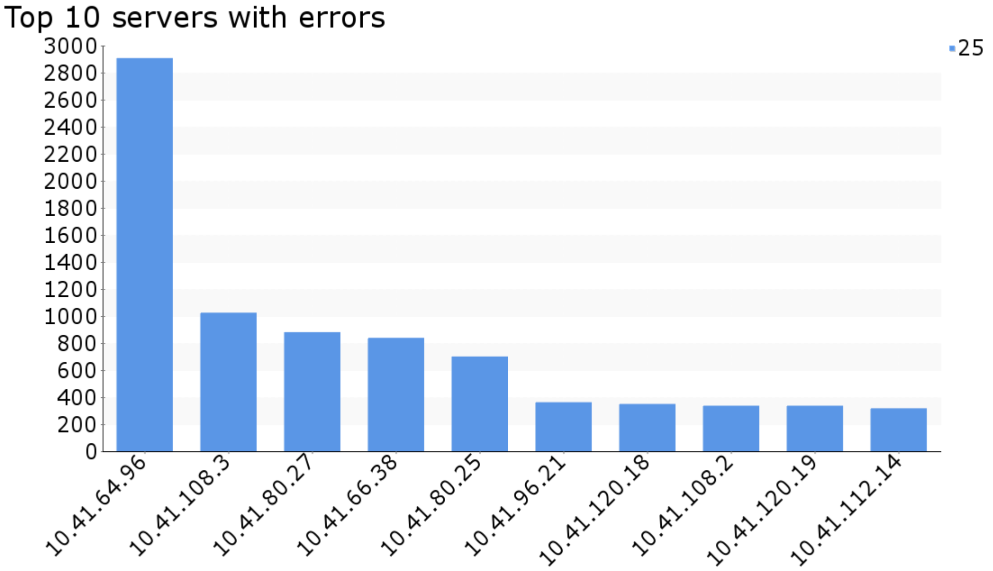
Note that the IP addresses are the In-path interfaces, this means that the same SteelHead can appear one or more times depending on how many interfaces it has.



Peer SH	25
192.168.62.7	3764
192.168.61.7	1597
192.168.61.40	1348
192.168.62.41	673
192.168.63.23	631
192.168.63.56	618
192.168.63.41	528
192.168.61.21	250

Top 10 servers with errors

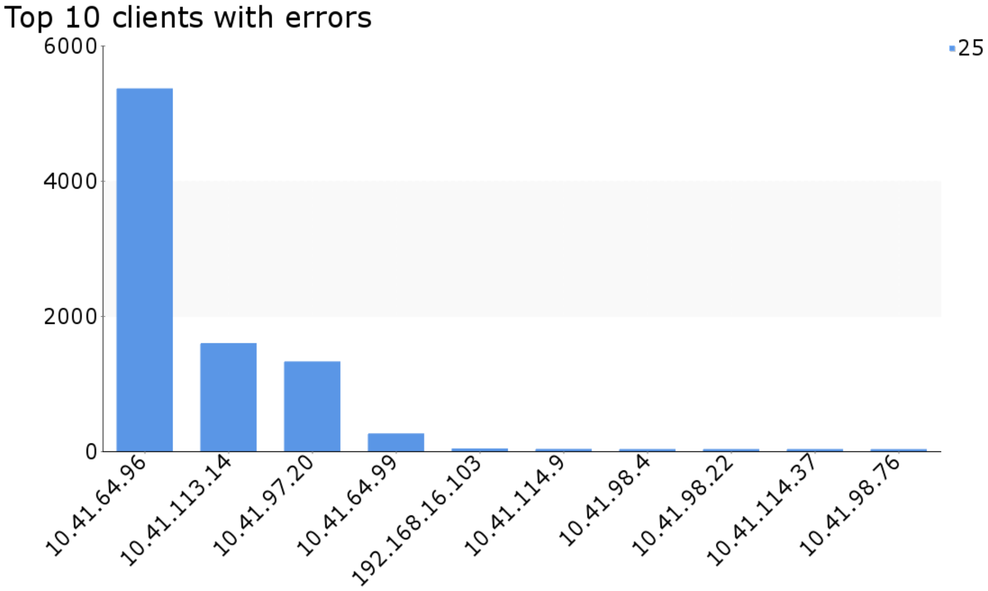
Within this section of the report we identify the servers causing the issues. Furthermore you can use this section to prioritize between servers/locations that have higher business priority.



Server IP	25
10.41.64.96	2901
10.41.108.3	1018
10.41.80.27	874
10.41.66.38	832
10.41.80.25	694
10.41.96.21	356
10.41.120.18	343
10.41.108.2	330
10.41.120.19	330
10.41.112.14	311

Top 10 clients with errors

Within this section of the report we identify the clients that are causing issues. You can use this section to prioritize between clients/locations that have higher business priority.



Client IP	25
10.41.64.96	5353
10.41.113.14	1586
10.41.97.20	1315
10.41.64.99	250
192.168.16.103	28
10.41.114.9	21
10.41.98.4	19
10.41.98.22	19
10.41.114.37	19
10.41.98.76	18

Appendix

How we collect data and analyze

We collect data in several ways to provide the most comprehensive view of the SteelHeads performance, workload and efficiency. The primary method is CLI (Command Line Interface).
For connection data the SteelHead is instructed to transmit the details of currently open sessions - every 15 minutes. By automatically sampling for connection data per SteelHead, 24 hours a day, 7 days a week we build up the most detailed set of statistics possible, meaning that we can provide the most robust and valid analysis of this important performance metric.

In general an error amount below 5% should not be considered a problem.

Transport Error Codes

Transport error	Error description
1	No error. Possible configuration mismatch
2	SSL server is unknown or misconfigured at the server-side steelhead
3	Protocol format used by the connection is neither SSLv3 nor TLSv1
4	SSL server requests client authentication but either Client Certificate Support is turned off on server-side Steelhead or the negotiated protocol is not TLSv1.
5	Client and server are reusing a previous session unknown to our Steelhead appliances
6	Misconfiguration of inner SSL security between client-side and server-side Steelhead appliances
7	SSL handshake between server-side Steelhead appliance and server has failed
8	SSL handshake between server-side Steelhead appliance and client has failed
9	SSL handshake between client-side and server-side Steelhead appliances has failed
10	Common name of subject in the SSL certificate presented by the backend server is different from expected
11	Couldnt export the SSL session key/context for migration from server-side Steelhead appliance to client-side Steelhead appliance
12	Couldnt import the SSL session key/context obtained from server-side Steelhead appliance at the client-side Steelhead appliance
13	Renegotiation of an SSL session established already between server-side Steelhead appliance and the server
14	Renegotiation of an SSL session established already with the client
15	Unexpected inter-steelhead control message received by the peer appliance

16	Server-side steelhead is not configured for the advanced SSL mode of operation
17	Server-side steelhead is not configured for the traditional SSL mode of operation
18	Server-side steelhead instructed the client-side sport to bypass the connection
19	Peering trust is misconfigured on the server-side Steelhead
20	Unexpected data received from the server
21	Invalid or missing SSL license
22	No proxy certificate is configured for the server.
23	Inner channel is not secure
24	Server is already in the Discovered (bypassed, not optimizable) table on server-side Steelhead
25	SSL optimization is either disabled or not configured correctly
26	Client and Server negotiated a cipher incompatible with the Steelhead
27	SSL stream cipher and client authentication are incompatible with latency optimization
28	Server likely sent an Alert for TLS Extension in the Client Hello
29	The Server response is unexpected or unknown. e.g. anon DH-cipher type of handshake