

Trouble Groups

Published: 2018-02-06

A trouble group is a collection of devices that are exhibiting some form of potentially problematic behavior. The following trouble groups are automatically identified by the ExtraHop system.

Aborted HTTP/DB transactions

Aborted HTTP/DB transactions indicate a high level of aborts during active HTTP or database transactions. Aborts are generally initiated by clients, so this might indicate that the server hangs on the response or does not complete the response in a timely manner.

| | |
|------------------|--|
| Criteria | Check for high levels of Requests Aborted or Responses Aborted |
| Devices | Devices that show HTTP or DB server activity and are not gateways or load balancers |
| Update | Hourly |
| Remedial Actions | For HTTP transactions, check for URLs that take along time to process. For database transactions, check for long-running stored procedures |

ADC SNAT pool too small

ADC SNAT pool too small indicates that a connection failed to initiate because the current device interpreted the SYN as belonging to a previous connection.

| | |
|------------------|---|
| Criteria | Check for any PAWS-Dropped-SYNs (In) |
| Devices | Known ADCs only (based on MAC address OID lookup) |
| Update | Hourly |
| Remedial Actions | On the BIG-IP Application Delivery Controller (ADC), the SNAT pool size should be increased |

ADC TCP connection throttling

ADC TCP connection throttling indicates that the connections are stalling in the Application Delivery Controller (ADC) and it is unable to keep up with the rate of data sent.

| | |
|------------------|---|
| Criteria | Check for zero windows (out) as a factor of the number of established connections |
| Devices | Known ADCs only (based on MAC address OID lookup) |
| Update | Hourly |
| Remedial Actions | On the BIG-IP Application Delivery Controller (ADC), the proxy_buffer_high setting in the TCP profile should be increased |

Database server backups

Database server backups are caused by backups taking place over CIFS, NFS, or Veritas on active database servers.

| | |
|------------------|--|
| Criteria | Detect large amount of storage traffic exchanged from the server |
| Devices | Devices that show CIFS, NFS, or TCP port 13724 activity (Veritas) and are not gateways or load balancers |
| Update | Every 30 minutes |
| Remedial Actions | Throttle down backups and schedule them during times with lower traffic |

DNS missing entries

DNS missing entries might indicate a service availability problem.

| | |
|------------------|---|
| Criteria | Compare DNS NXDOMAINS responses with the total number of responses |
| Devices | Devices that show DNS server activity and are not gateways or load balancers |
| Update | Hourly |
| Remedial Actions | If these queries are intended, add an entry to DNS. If not, find the clients making erroneous DNS requests and configure them to stop making these requests |

Excessive HTTP authorizations

Excessive HTTP authorizations should be checked for large numbers of HTTP authorization errors, which might indicate break-in attempts.

| | |
|------------------|---|
| Criteria | Check for 401 errors and compare them with the number of valid responses |
| Devices | Devices that show HTTP server activity and are not gateways or load balancers |
| Update | Hourly |
| Remedial Actions | Log these HTTP authorization errors, as these errors might indicate break-in attempts |

HTTP broken links

HTTP broken links indicate that a resource has been moved or deleted but the document might still points to the old location.

| | |
|----------|---|
| Criteria | Check for 404s and compare it with the number of valid responses |
| Devices | Devices that show HTTP server activity and are not gateways or load balancers |
| Update | Hourly |

| | |
|------------------|-------------------------------|
| Remedial Actions | Track down the source of 404s |
|------------------|-------------------------------|

Path MTU mismatch

Path MTU mismatch displays the list of devices for which path MTU mismatch was detected. These devices are not respecting the Fragmentation Needed ICMP announcements.

| | |
|------------------|--|
| Criteria | Check for ICMP type 3 code 4 |
| Devices | All devices |
| Update | Hourly |
| Remedial Actions | Check documentation for devices that are not respecting path MTU announcements for configuration options |

Problematic TCP offloading engine

Problematic TCP offloading engine. Indicates that the current device is sending too much data resulting in network congestion and dropped packets. This behavior has been seen with a number of TCP offloading engines.

| | |
|------------------|---|
| Criteria | Check for Bad Congestion Control (Out) |
| Devices | NICs known to have problems (based on MAC address OID lookup) |
| Update | Hourly |
| Remedial Actions | Turn off TCP offloading |

Server TCP connection throttling

Server TCP connection throttling is caused by server running out of buffer or CPU resources and throttling network connections as a result.

| | |
|------------------|---|
| Criteria | Check for the zero windows (out) as a factor of the number of established connections |
| Devices | Devices that are servers and are not gateways or load balancers |
| Update | Every 30 minutes |
| Remedial Actions | Check buffer sizes and CPU, and increase those resources, if necessary |

SPAN oversubscription

SPAN oversubscription indicates that data coming over the SPAN port is incomplete. This can happen to data being dropped at the SPAN port due to oversubscription or microbursts.

| | |
|----------|---|
| Criteria | Compare the desyncs to the number established connections |
| Devices | All devices |
| Update | Daily |

| | |
|------------------|---|
| Remedial Actions | Filter down data coming over the SPAN port or use a larger capacity SPAN port |
|------------------|---|

SSL Key Size < 2048

SSL key size < 2048 indicates a 1024-bit SSL key. In 2010, 1024-bit public keys have been declared insecure by NIST. As a result, certificate authorities are moving to 2048-bit keys.

| | |
|------------------|--|
| Criteria | Check for SSL public key size less than 2048 bits |
| Devices | Devices that show SSL server activity and are not gateways |
| Update | Hourly |
| Remedial Actions | Deploy 2048-bit keys in place of potentially insecure ones |

Virtual packet loss

Virtual packet loss indicates that a virtual instance is overwhelmed and cannot send packets out in a timely fashion. TCP interprets delayed ACKs as packet loss and sends less data.

| | |
|------------------|---|
| Criteria | Check for large numbers of RTOs coming from devices within virtualized environments |
| Devices | Virtualized devices (based on MAC address OID lookup) |
| Update | Hourly |
| Remedial Actions | Provide more hardware resources to stressed VMs |