

DOMAIN NAME SYSTEM



QPS &
Benchmark
Report
Document



sales@advantal.net
www.advantaltechnologies.com



TABLE OF CONTENTS

1. Introduction.....3

2. Node-Level Capacity Overview.....3

3. Node-Level Throughput Benchmark (Per Appliance).....4

3.1 Authoritative Throughput.....4

3.2 Recursive Throughput.....5

4. DNSSEC Performance.....5

5. Virtualized Deployment Performance.....6

6. Latency Metrics.....6

7. Performance Under Full Security Load.....6

8. High-Level Summary of Performance.....7

9. Conclusion.....8

1. INTRODUCTION

This Performance Benchmark Report summarizes the **node-level (per appliance) DNS throughput** for key workloads—**Authoritative, Recursive/Caching, DNSSEC**, and **Virtualized (VM)**—as committed in the OEM/Bidder response matrix. It also defines a practical benchmark approach and compliance interpretation for customer validation.

Key definitions (used throughout this report):

- **Per node / per appliance:** Performance measured for a single DNS appliance instance.
- **Sustained QPS:** Throughput maintained continuously (24×7) during steady-state workload without degradation or unacceptable error/timeout rates.
- **Peak QPS:** Maximum burst capacity under tuned conditions and adequate headroom.
- **N+1 Active-Active HA:** Cluster design where total required QPS is maintained even if one node fails.

2. NODE-LEVEL CAPACITY OVERVIEW

The following values represent the committed per node / per appliance performance envelope:

Parameter	Committed Capacity (Per Node / Appliance)	Compliance Statement
Licensed QPS per node	500,000 QPS	Meets licensed baseline capacity per node.
Sustained QPS (Authoritative)	≥ 500,000 QPS (24×7)	Meets sustained authoritative requirement per node under authoritative workload.
Sustained QPS (Recursive/Caching)	150,000 – 200,000 QPS	Meets sustained recursive capacity per node under mixed recursive workload.
Peak QPS	Up to 1,000,000 QPS	Meets peak burst capacity per node under tuned conditions.
DNSSEC QPS (Authoritative DNSSEC)	250,000 – 320,000 QPS	Meets authoritative DNSSEC throughput per node reflecting crypto overhead.
VM QPS range	80,000 – 350,000 QPS	Meets VM throughput range depending on allocated resources.

Parameter	Committed Capacity (Per Node / Appliance)	Compliance Statement
Max QPS per appliance (Top-end)	1,000,000 QPS	Scalable to 1M QPS per appliance without hardware change (as committed).
Cluster-wide scaling	Linear by adding nodes; N+1 Active-Active HA	Meets scalability and resilience requirement; throughput maintained on single node failure.

3. NODE-LEVEL THROUGHPUT BENCHMARK (PER APPLIANCE)

3.1 AUTHORITATIVE THROUGHPUT

Committed per-node authoritative sustained throughput:

- **≥ 500,000 QPS per appliance**, sustained **24×7** under authoritative DNS workload.

Committed per-node authoritative peak throughput:

- **Up to 1,000,000 QPS per appliance** under peak/burst conditions.

Compliance interpretation (authoritative):

- The solution is compliant with a per-node sustained baseline of **500k QPS** for authoritative traffic.
- Peak capability per node is committed at **1M QPS**, suitable for burst handling and traffic spikes.
- For HA compliance, the architecture must ensure that during a single-node outage, the remaining nodes sustain the required site QPS (N+1).

3.2 RECURSIVE THROUGHPUT

Committed per-node recursive/caching sustained throughput:

- **150,000 – 200,000 QPS per appliance** under **mixed recursive workload**.

Compliance interpretation (recursive):

- The solution is compliant with per-node recursive throughput in the range **150k–200k QPS**.
- Recursive throughput is inherently workload-dependent (cache-hit ratio, upstream latency, query variety). The committed range reflects a “mixed” real-world profile rather than best-case cache-only conditions.

Operational notes (benchmark expectations):

- To validate correctly, recursive tests should define:
- Cache hit ratio (e.g., warm cache + controlled misses),
- Upstream dependency behavior,
- EDNS0/TCP fallback behavior (if relevant).

4. DNSSEC PERFORMANCE

Committed per-node authoritative DNSSEC throughput:

- **250,000 – 320,000 QPS per appliance** for **Authoritative DNSSEC**.

Compliance interpretation (DNSSEC):

- The solution is compliant for DNSSEC-signed authoritative zones at **250k–320k QPS per node**.
- The matrix explicitly recognizes DNSSEC overhead (crypto + larger responses). Practically, DNSSEC throughput is expected to be lower than non-DNSSEC authoritative throughput.

Sizing implication (per-node planning):

- If a site requires **500,000 QPS under DNSSEC**, the design should consider **multiple nodes** to meet sustained requirements with headroom.
- For N+1 resilience under DNSSEC workloads, design should include an additional node beyond the required active count.

5. VIRTUALIZED DEPLOYMENT PERFORMANCE

Committed per-VM throughput range:

- **80,000 – 350,000 QPS per virtual appliance**, dependent on **vCPU, RAM, NIC allocation**, and virtualization/network path.

Compliance interpretation (VM):

- The solution is compliant for virtualized deployments within the stated throughput envelope, provided resources are sized appropriately.

6. LATENCY METRICS

The provided matrix is QPS-focused and does **not** define explicit latency numbers. Therefore, latency must be treated as a **measured acceptance metric** during benchmark execution.

Recommended latency metrics to capture (per node, per scenario):

- **p50 latency (median)**
- **p95 latency**
- **p99 latency**
- **Timeout rate (%)**
- **Error response rate (%)** (SERVFAIL, FORMERR, etc.)

Compliance statement (latency):

- Latency will be reported as part of benchmark evidence and must remain stable while sustaining the committed QPS levels for the relevant workload (authoritative / recursive / DNSSEC / VM).

7. PERFORMANCE UNDER FULL SECURITY LOAD

“Full security load” typically includes **DNSSEC**, policy controls, and operational logging/telemetry. While the matrix explicitly provides DNSSEC throughput, additional security features can introduce overhead depending on configuration.

Committed baseline under DNSSEC security condition (authoritative):

- **250,000 – 320,000 QPS per node** (Authoritative DNSSEC)

Security-load validation scope (recommended for compliance):

- DNSSEC-enabled signed zones (authoritative)
- Rate limiting / anti-abuse controls (if enabled)
- Access policy controls (if enabled)
- Logging/metrics enabled in production-safe mode

Compliance statement (security load):

- Under DNSSEC-enabled authoritative operation, the solution sustains the committed throughput range (**250k–320k QPS per node**) and will provide benchmark evidence for CPU/NIC headroom and error/timeout stability.

8. HIGH-LEVEL SUMMARY OF PERFORMANCE

Per-node committed performance summary (compliance-ready):

- **Licensed baseline per node: 500,000 QPS**
- **Sustained authoritative per node (24×7): $\geq 500,000$ QPS**
- **Recursive/caching per node: 150,000–200,000 QPS**
- **Peak per node: Up to 1,000,000 QPS**
- **Authoritative DNSSEC per node: 250,000–320,000 QPS**
- **VM per instance: 80,000–350,000 QPS**
- **Scale per appliance (top-end): 1,000,000 QPS without hardware change**
- **Cluster scalability:** Linear by adding nodes + **N+1 active-active HA** ensures service continuity and required QPS during single node failure.

Cluster compliance statement (N+1):

- The architecture is designed to **maintain required QPS during a single node or hardware failure**, by distributing load across active-active nodes and keeping **one additional node** beyond the required active capacity.

9. CONCLUSION

Based on the OEM/Bidder QPS matrix, the solution is compliant **per node / per appliance** for:

- **≥ 500,000 QPS sustained authoritative (24×7),**
- **150,000–200,000 QPS sustained recursive,**
- **250,000–320,000 QPS authoritative DNSSEC,**
- **Up to 1,000,000 QPS peak, and 1,000,000 QPS top-end per appliance** (scalable without hardware change),
- plus **linear scale-out and N+1 active-active HA** to maintain required throughput during a node failure.

For acceptance, the benchmark should include QPS evidence **per workload**, along with latency (p50/p95/p99) and error/timeout stability, as environment-specific proof supporting the committed capacity envelope.





EXPERIENCE ADVANTAL DNS IN ACTION

Scan to Request a Free Demo



Talk to our experts and discover how automated, secure, and high-performance DNS can modernize your entire network stack.

Advantal Technologies Limited
(Make In India OEM)

-  sales@advantal.net
-  kartikay.shukla@advantal.net
-  +91 99711 61261
-  www.advantaltechnologies.com

EAL2+, NDPP, NDcPP Certified