CHECKLIST

DNSSEC Validation Failures Troubleshooting Checklist

A practical, vendor-neutral checklist for identifying where DNSSEC validation fails, confirming the chain of trust, and choosing the right remediation path across the zone, registrar, and resolver.

DNSSEC Validation Failures: Troubleshooting Checklist

Use this checklist to quickly localize DNSSEC validation failures and determine whether the fix belongs in the authoritative zone, parent delegation/registrar, or recursive resolver.

---

1) Confirm the failure is actually DNSSEC validation

- [ ] Compare the failing query against at least two resolvers:
- [ ] One known-validating resolver
- [ ] One resolver that does not validate, if available
- [ ] Note the exact client symptom:
- [ ] SERVFAIL
- [ ] Intermittent resolution failure
- [ ] Failure only for specific record types
- [ ] Failure only in one network, site, or application
- [ ] Verify whether the authoritative server is answering normally
- [ ] Confirm whether the failure appears only for validating resolvers
- [ ] Distinguish DNSSEC validation failure from policy-based blocking or filtering

If non-validating resolvers succeed but validating resolvers fail, DNSSEC is likely involved.

---

2) Identify where the chain of trust breaks

- [ ] Verify the resolver has a valid trust anchor
- [ ] Confirm the resolver is attempting to validate DNSSEC
- [ ] Check that the parent zone publishes a DS record for the child zone
- [ ] Check that the child zone publishes a DNSKEY that matches the DS digest
- [ ] Confirm the RRset being queried has a current RRSIG
- [ ] Confirm the signature validity window is current
- [ ] Check for missing delegation data, lame servers, or inconsistent authoritative answers

Healthy chain of trust: Root trust anchor ? parent DS ? child DNSKEY ? signed RRset ? validated answer

---

3) Check the most common failure patterns

SERVFAIL from validating resolvers

- [ ] Compare results from validating and non-validating resolvers
- [ ] Look for DS/DNSKEY mismatch
- [ ] Check for expired or missing RRSIGs
- [ ] Check delegation consistency and glue records
- [ ] Review NSEC/NSEC3 proofs for negative responses

Intermittent failures

- [ ] Check for stale cached data
- [ ] Inspect signature expiration timing
- [ ] Look for partial propagation during key rollover
- [ ] Compare responses from multiple authoritative servers
- [ ] Verify clock synchronization on signing systems

Failure only for one record type or subdomain

- [ ] Confirm whether only one RRset is unsigned or unsigned after change
- [ ] Check whether the signing pipeline included all record types
- [ ] Verify delegated child zones are signed and aligned with parent delegation

Internal clients fail but external clients work

- [ ] Compare internal and external resolver behavior
- [ ] Check for split-horizon DNS
- [ ] Review forwarding rules and security policies
- [ ] Confirm whether one resolver validates DNSSEC and another does not

---

4) Verify the authoritative zone

- [ ] Confirm the zone is fully signed
- [ ] Check that all required RRsets have RRSIGs
- [ ] Verify signature inception and expiration timestamps

- [ ] Check for clock drift on signing infrastructure
- [ ] Confirm DNSKEY records are present and current
- [ ] Verify that changes were signed before publication
- [ ] Check that inline or offline signing completed successfully
- [ ] Inspect NSEC/NSEC3 records for correct denial-of-existence coverage

Authoritative-zone indicators:

- Expired signatures
- Missing signatures after updates
- Partial signing
- Bad NSEC/NSEC3 data
- Inconsistent answers across authoritative servers

---

5) Verify the parent delegation and registrar path

- [ ] Confirm the parent zone publishes the correct DS record
- [ ] Confirm the DS digest matches the current child DNSKEY
- [ ] Check whether a key rollover is in progress
- [ ] Verify the old DNSKEY was not removed too early
- [ ] Verify the new DS was not published before the child key was active
- [ ] Confirm delegation NS records are correct and consistent
- [ ] Check glue records if the nameservers are in-bailiwick
- [ ] Verify all authoritative servers serve the same DNSSEC data

Parent/delegation indicators:

- DS and DNSKEY mismatch
- Broken delegation
- Stale or missing glue
- Inconsistent authoritative servers

- Key rollover timing errors

---

6) Verify the recursive resolver path

- [ ] Confirm whether the resolver is validating DNSSEC
- [ ] Check whether a forwarder or upstream resolver is involved
- [ ] Review resolver logs or validation status for exact failure codes
- [ ] Confirm the trust anchor configuration
- [ ] Check for local policy that converts validation failures into hard errors
- [ ] Verify the resolver is not using stale cache data
- [ ] Confirm the resolver is not bypassing validation in one environment and enforcing it in another

Resolver-path indicators:

- Validation disabled or inconsistent
- Wrong trust anchor
- Policy override
- Forwarding misconfiguration
- Resolver-specific SERVFAIL behavior

---

7) Isolate the failure safely

- [ ] Test an existing name and a nonexistent name
- [ ] Compare positive and negative responses
- [ ] Query each authoritative server directly
- [ ] Compare results before and after cache expiry
- [ ] Test both apex and delegated child names

- [ ] Repeat from multiple network locations if possible

Interpretation tips:

- Existing names fail only: likely signing or chain issue for the RRset
- Nonexistent names fail only: likely NSEC/NSEC3 problem
- One authoritative server differs: likely deployment inconsistency
- One resolver differs: likely resolver configuration or policy issue

---

8) Decide where the fix belongs

Fix in the zone when:

- [ ] RRSIGs are expired or missing
- [ ] DNSKEYs are stale or incorrect
- [ ] New records were published before signing completed
- [ ] NSEC/NSEC3 records are wrong or incomplete

Fix in the registrar or parent delegation when:

- [ ] DS does not match the child DNSKEY
- [ ] Delegation NS records are wrong
- [ ] Glue is missing or stale
- [ ] A key rollover was published out of sequence

Fix in the resolver when:

- [ ] Validation is disabled or inconsistent

- [ ] Trust anchors are wrong or outdated
- [ ] Forwarding changes behavior unexpectedly
- [ ] Policy rules override normal validation results

---

9) Validate the remediation

- [ ] Re-test the same query from a validating resolver
- [ ] Confirm SERVFAIL is gone
- [ ] Confirm both positive and negative responses validate
- [ ] Confirm multiple record types validate successfully
- [ ] Confirm all authoritative servers answer consistently
- [ ] Confirm the fix persists after cache refresh
- [ ] Document the root cause and the remediation path

Quick triage summary

- [ ] DS/DNSKEY mismatch ? check parent delegation and key rollover timing
- [ ] Expired signatures ? check signing jobs and clocks
- [ ] Missing signatures ? check signing pipeline and zone publication order
- [ ] Broken delegation ? check NS, glue, and authoritative consistency
- [ ] NSEC/NSEC3 failure ? test negative responses and zone denial records
- [ ] Resolver policy issue ? check validation settings and trust anchors

---

Notes for incident response

- [ ] Capture the failing name, record type, resolver IP, and timestamp
- [ ] Save the exact error message or response code
- [ ] Record whether the resolver validates DNSSEC
- [ ] Note whether the issue affects all clients or only one network segment
- [ ] Keep changes minimal until the failure point is confirmed

---

Final check before closing the incident

- [ ] The chain of trust validates end to end
- [ ] The authoritative zone is signed correctly
- [ ] The parent DS record matches the child DNSKEY
- [ ] The resolver is validating as expected
- [ ] The fix was applied in the correct layer

If all items are checked, the DNSSEC validation issue is likely resolved.