CHECKLIST

DNSSEC Deployment Best Practices Checklist

A practical, vendor-neutral checklist to help teams deploy DNSSEC safely, verify trust-chain integrity, and avoid validation-related outages.

DNSSEC Deployment Best Practices Checklist

Use this checklist to prepare, deploy, and validate DNSSEC in production environments. It is designed for operators who need to maintain a working trust chain from the root to the signed zone while minimizing the risk of validation failures.

1) Confirm readiness before enabling DNSSEC

- [ ] Confirm your authoritative DNS platform supports DNSSEC signing and the key algorithms you plan to use.
- [ ] Confirm your registrar or parent-zone workflow supports DS record publication and updates.
- [ ] Verify that validating resolvers in your environment can perform DNSSEC validation.
- [ ] Identify which resolver paths are validating, forwarding, or non-validating.
- [ ] Document all zones, subzones, and delegations that may be affected.
- [ ] Confirm operational ownership for zone signing, registrar changes, and resolver policy.
- [ ] Define a rollback plan before making any DNSSEC changes.
- [ ] Establish maintenance windows that account for DNS cache timing and signature refresh intervals.

2) Design the signing and rollover strategy

- [ ] Choose the smallest practical set of signing keys for the zone.
- [ ] Decide which key rollover method will be used and who approves it.
- [ ] Document the timing for key introduction, key retirement, and signature refresh.
- [ ] Confirm that signature validity periods align with refresh and propagation behavior.
- [ ] Verify that key management procedures are repeatable and auditable.
- [ ] Make sure old and new keys can coexist long enough for a safe transition.
- [ ] Identify any automation used for signing, re-signing, or DS updates.
- [ ] Test the rollover process in a non-production environment first if possible.

3) Sign the zone correctly

- [ ] Sign the zone on the authoritative side before publishing DS records.
- [ ] Confirm the DNSKEY set is present and current.
- [ ] Verify that all intended records are signed.
- [ ] Check that no critical records are excluded from signing accidentally.
- [ ] Validate that NSEC or NSEC3 behavior matches your operational and privacy requirements.
- [ ] Ensure signature inception and expiration values are valid and consistent.
- [ ] Confirm the signed zone loads correctly on all authoritative servers.
- [ ] Verify that zone transfers, replication, and backups preserve DNSSEC metadata.

4) Verify delegation and chain of trust

- [ ] Publish the correct DS record at the parent or registrar.
- [ ] Confirm the DS record matches the child zone DNSKEY set.

- [ ] Check that DS key tag, algorithm, and digest type are correct.
- [ ] Verify the delegation chain from the resolver to the signed zone.
- [ ] Confirm that the parent-child relationship is visible to validating resolvers.
- [ ] Test validation from multiple resolver implementations.
- [ ] Test validation from multiple networks or geographic locations if relevant.
- [ ] Ensure no stale DS record remains after a key change.
- [ ] Confirm that the chain remains intact after propagation delays and cache refreshes.

5) Validate from the resolver layer you actually depend on

- [ ] Test internal validating resolvers.
- [ ] Test public resolvers used by remote staff, customers, or applications.
- [ ] Test any recursive resolvers behind application platforms.
- [ ] Compare behavior between validating and non-validating resolvers.
- [ ] Confirm whether each resolver path validates independently or forwards upstream responses.
- [ ] Look for SERVFAIL responses on signed zones.
- [ ] Check for intermittent failures caused by cache timing.
- [ ] Verify that test lookups succeed consistently, not just once.
- [ ] Capture the exact resolver path used when problems appear.

6) Monitor for common failure conditions

- [ ] Alert on SERVFAIL spikes for signed zones.
- [ ] Monitor for DNSKEY and DS mismatches.
- [ ] Track signature expiration and near-expiration conditions.
- [ ] Watch for authoritative server misconfiguration after any update.

- [ ] Check for broken delegation after registrar changes.
- [ ] Monitor for resolver policy differences across locations.
- [ ] Review cache behavior after every signing or rollover change.
- [ ] Distinguish validation failures from general DNS outages.
- [ ] Keep a record of the first resolver path where failure appears.

7) Control change management tightly

- [ ] Treat DS publication as a production security change.
- [ ] Require approval for key rollovers and trust-anchor changes.
- [ ] Keep zone signing, resolver updates, and registrar updates coordinated.
- [ ] Avoid making unrelated DNS changes during DNSSEC rollout.
- [ ] Record who made each change and when it was applied.
- [ ] Confirm that registrar workflows complete successfully before closing the change.
- [ ] Notify all affected teams before rotation or expiry events.
- [ ] Re-verify validation after any emergency or out-of-band edit.

8) Prepare safe rollback options

- [ ] Define how to temporarily disable validation impact if needed.
- [ ] Keep prior keys or prior trust data available during transition windows.
- [ ] Know how to remove or replace a broken DS record quickly.
- [ ] Document the conditions that require rollback versus repair.
- [ ] Test rollback in a controlled environment if possible.
- [ ] Ensure rollback steps are available to all responsible operators.
- [ ] Confirm that rollback actions will not create a second trust-chain failure.
- [ ] Validate service recovery after rollback, not just configuration changes.

9) Confirm production readiness

- [ ] The zone is signed and published correctly.
- [ ] The DS record matches the child DNSKEY set.
- [ ] Multiple validating resolvers can chain trust successfully.
- [ ] No critical resolver path returns SERVFAIL for the signed zone.
- [ ] Monitoring is in place for signature expiry and validation failures.
- [ ] Key rollover responsibilities are assigned and documented.
- [ ] Rollback steps are ready and tested.
- [ ] The rollout has been verified from every resolver path that matters.

10) Post-deployment review

- [ ] Review logs for validation errors after the change window.
- [ ] Confirm cached data has fully transitioned to the new trust state.
- [ ] Check whether any resolver population still uses stale or broken configuration.
- [ ] Document lessons learned for future key rotations.
- [ ] Update runbooks with the actual resolver paths and validation behavior observed.
- [ ] Record any follow-up work needed for resolver upgrades or registrar process changes.

Quick go-live checklist

- [ ] Authoritative DNS supports the planned DNSSEC model.
- [ ] Registrar/parent can publish the required DS record.
- [ ] The zone is correctly signed.
- [ ] Validating resolvers successfully verify the trust chain.
- [ ] Monitoring and alerting are active.

- [ ] Rollback steps are documented and accessible.
- [ ] Change ownership is clear across DNS, registrar, and resolver teams.

Notes for operators

- DNSSEC improves authenticity, not confidentiality.
- A signed zone is not ready for production until validating resolvers can verify it consistently.
- Most DNSSEC failures are caused by timing, delegation, or coordination mistakes rather than signature generation itself.
- When in doubt, verify the full chain of trust from resolver to parent to child zone before declaring success.