**BIND's Default Policy for Recursion**

In versions of BIND prior to (and including) BIND 9.4.1, the default behavior of BIND servers was to allow recursion for all clients unless otherwise specified.  
  
Because open recursion has some undesirable side-effects, such as allowing a server to be exploited by attackers targeting a victim with DNS amplification attacks, the default behavior was changed in BIND 9.4.1-P1.  Since 9.4.1-P1, unless an ACL is explicitly specified in the "allow-recursion" statement, the default access list is set to "localnets; localhost;" - in other words, the local server machine and those broadcast domains for which the server has a network interface configured at the time named is started.  
  
ISC no longer supports versions of BIND prior to 9.9, but some OS vendors still distribute their own BIND packages based on versions that are no longer supported.  If you are running such a version our advice is to upgrade to [**any currently supported version**](https://www.isc.org/downloads/), but if you cannot, you can limit recursion by specifying the addresses or networks you wish to allow.  Example syntax can be found in the article below.

**Following is our original ISC article from the time of the change in default behavior.**

There has been some confusion surrounding the changes to the "allow-recursion" and "allow-query-cache" options made with BIND 9.4.1-P1.

This document will attempt to clarify the change and the impact that it makes on BIND servers.

In BIND 9.3, there was no segregation of queries between cache and authoritative data.

The release of BIND 9.4 added fine-grained differentiation between queries against authoritative data ("allow-query") and cached data ("allow-query-cache"). This allows more precise control, particularly if you do not want your clients to use any cached data, for example, in an authoritative-only nameserver.

Prior to the release of BIND 9.4.1-P1, the default action of  
"allow-recursion" and "allow-query-cache" was to permit the query. The P1 patch to BIND 9.4.1 caused two changes in this behavior:

1. If not explicitly set, the ACLs for "allow-query-cache" and "allow-recursion" were set to "localnets; localhost;".
2. If either "allow-query-cache" or "allow-recursion" was set, the other would be set the same value.

Upgrading from the BIND 9.3 branch to BIND 9.4.1-P1 will  
significantly restrict those servers that were previously recursive servers for more than "localhost; localnets;" unless configuration changes are made.

To retain the behavior prior to BIND 9.4.1-P1, the following entries would need to be added to your named.conf file:

options {

...

allow-recursion { any; };

allow-query { any; };

allow-query-cache { any; };

...

};

Shell

Copy

However, we **strongly advise against** this configuration because clients spoofing queries can use your servers to launch distributed denial-of-service attacks.

**The recommended method** is to create ACLs that match hosts that should be allowed access to cache and recursion on the servers. For example, if you wanted to provided recursion and access to the cache to clients you trusted, you could list them in an ACL such as the following:

acl "trusted" {

192.168.0.0/16;

10.153.154.0/24;

localhost;

localnets;

};

options {

...

allow-query { any; };

allow-recursion { trusted; };

allow-query-cache { trusted; };

...

};

Shell

Copy

This example ACL includes 192.168.0.0/16 and 10.153.154.0/24 as sample networks that would require access. You must replace these sample networks with networks that correctly reflect your environment. This will allow anyone to query your server for authoritative data, but only those hosts within the "trusted" ACL access to your cache and recursion.

**How do I change the version that BIND reports when queried for version.bind?**

* Updated On 15 Oct 2018
* 1 Minute To Read
* Contributors

[](https://kb.isc.org/docs/author/suzanne)[](https://kb.isc.org/docs/author/isc)

* Print
* Share
* Dark

BIND servers respond to queries for name **version.bind** with record type **TXT** and class **CHAOS**. By default this is set to the version of BIND that has been installed.

dig @127.0.0.1 version.bind chaos txt

; <<>> DiG 9.11.0 <<>> @127.0.0.1 version.bind chaos txt

; (1 server found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22214

;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; WARNING: recursion requested but not available

;; QUESTION SECTION:

;version.bind. CH TXT

;; ANSWER SECTION:

version.bind. 0 CH TXT "9.11.0"

;; AUTHORITY SECTION:

version.bind. 0 CH NS version.bind.

;; Query time: 160 msec

;; SERVER: 127.0.0.1#53(127.0.0.1)

;; WHEN: Wed Mar 15 15:07:34 2017

;; MSG SIZE rcvd: 63

Shell

Copy

Sometimes it is desirable not to reveal the version of BIND that is running on the server. The default version can be changed using the **version** option in the **options** statement in **named.conf**. For example:

version "BIND 9";

Shell

Copy

It's also possible to disable version reporting entirely:

version none;