

BIND9 DNS- Samba AD

-
- Bind
- BIND
 - localhost 0.0.127.in-addr.arpa
 -
 - / BIND
 - - localhost
 - 0.0.127.in-addr.arpa.
- BIND9_DLZ
- /usr/sbin/samba_dnupdate: ; TSIG error with server: tsig verify failure
- "status: FORMERR" DNS- Windows AD

 wiki.samba.org
 , Bind9.

, Samba Active Directory (AD), DNS-
Astra Linux DNS- BIND9, .

BIND9, , , Samba AD DC.
DNS Samba Bind9 . [DNS](#) [AD Samba](#).

Bind

bind c. [DNS- BIND9](#)

BIND

 AD named.conf , AD.

localhost 0.0.127.in-addr.arpa
localhost 0.0.127.in-addr.arpa (/etc/bind/db.local /etc/bind/db.127).

/ BIND

```
sudo systemctl start bind9
sudo systemctl restart bind9
```

DNS (127.0.0.1).

localhost

:

```
host -t A localhost 127.0.0.1
```

:

 Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
localhost has address 127.0.0.1

0.0.127.in-addr.arpa.

:

```
host -t PTR 127.0.0.1 127.0.0.1
```

:

 Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
1.0.0.127.in-addr.arpa domain name pointer localhost.

BIND9_DLZ

 Samba AD, /var/lib/samba/bind-dns/named.conf .

Samba AD /var/lib/samba/bind-dns/named.conf BIND9:

```
# This DNS configuration is for BIND 9.8.0 or later with dlz_dlopen support.
#
# This file should be included in your main BIND configuration file
#
# For example with
# include "/var/lib/samba/bind-dns/named.conf";
#
# This configures dynamically loadable zones (DLZ) from AD schema
# Uncomment only single database line, depending on your BIND version
#
dlz "AD DNS Zone" {
    # For BIND 9.8.x
    # database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9.so";

    # For BIND 9.9.x
    # database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_9.so";

    # For BIND 9.10.x
    # database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_10.so";

    # For BIND 9.11.x
    database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_11.so";
};
```

BIND9_DLZ:

/etc/bind/named.conf samba:

 include "/var/lib/samba/bind-dns/named.conf";

bind :

```
sudo named -v
```

, /var/lib/samba/bind-dns/named.conf , BIND. BIND 9.11.

/var/lib/samba/bind-dns/named.conf:

```
sudo chown -R root:bind /var/lib/samba/bind-dns/
```

:

```
sudo named-checkconf
```

bind9:

```
sudo systemctl restart bind9
```

/usr/sbin/samba_dnsupdate: ; TSIG error with server: tsig verify failure

"/usr/sbin/samba_dnsupdate: update failed: REFUSED" DNS .

"status: FORMERR" DNS- Windows AD

:

```
i dig SRV _ldap._tcp.windomain.ru
; <<>> DiG 9.11.3-1ubuntu1.5-Debian <<>> SRV _ldap._tcp.windomain.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: FORMERR, id: 16281
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: ad69f89824966028 (echoed)
;; QUESTION SECTION:
;_ldap._tcp.windomain.ru. IN SRV

;; Query time: 0 msec
;; SERVER: 10.0.2.10#53(10.0.2.10)
;; WHEN: Fri Dec 06 08:52:19 MSK 2019
;; MSG SIZE rcvd: 64
```

- , DNS- Windows AD, , ().

- dig +nocom cookie (+noends):

```
dig SRV _ldap._tcp.windomain.ru +nocom cookie
```

```
; <<>> DiG 9.11.3-1ubuntu1.5-Debian <<>> SRV _ldap._tcp.windomain.ru +nocom cookie
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46065
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;_ldap._tcp.windomain.ru. IN SRV

;; ANSWER SECTION:
_ldap._tcp.windomain.ru. 600 IN SRV 0 100 389 swin.windomain.ru.
_ldap._tcp.windomain.ru. 900 IN SRV 0 100 389 ad.windomain.ru.
```

```
;; ADDITIONAL SECTION:  
swin.windomain.ru. 3600 IN A 10.0.2.10  
ad.windomain.ru. 900 IN A 10.0.2.250  
  
;; Query time: 0 msec  
;; SERVER: 10.0.2.10#53(10.0.2.10)  
;; WHEN: Fri Dec 06 08:58:06 MSK 2019  
;; MSG SIZE rcvd: 156
```