

Modificam regulile de securitate astfel incat sa permitem trafic TCP/UDP pe portul 53.

Dam click pe **Security groups** (vezi sageata)

The screenshot shows the AWS CloudFormation console interface for a stack named 'subnet-07acb046648226588'. The 'Security' tab is highlighted with a red circle. Below it, the 'Security details' section is expanded, showing the IAM Role (empty), Owner ID (605102421104), and Launch time (Sat Mar 05 2022 23:42:07 GMT+0200 (Eastern European Standard Time)). The 'Security groups' section is also expanded, showing a single entry: 'sg-0991a6b817543b850 (launch-wizard-1)'. A red arrow points to this link. The 'Inbound rules' section is shown below, with a table listing one rule: sgr-0ba62ce013310cbde, Port range 22, Protocol TCP, Source 0.0.0.0/0, and Security group launch-wizard-1. A search bar labeled 'Filter rules' and navigation arrows are also visible.

Security group rule ID	Port range	Protocol	Source	Security groups
sgr-0ba62ce013310cbde	22	TCP	0.0.0.0/0	launch-wizard-1

Ne aflam in **Security groups** si editam **inbound rules** unde deja exista permis traficul SSH / TCP port 22.

**Details**

Security group name <a href="#">launch-wizard-1</a>	Security group ID <a href="#">sg-0991a6b817543b850</a>	Description <a href="#">launch-wizard-1 created 2022-03-05T23:41:14.046+02:00</a>	VPC ID <a href="#">vpc-098b33f68fe620354</a>
Owner <a href="#">605102421104</a>	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

[Inbound rules](#)   [Outbound rules](#)   [Tags](#)

(i) You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#) [X](#)

**Inbound rules (1/1)** [C](#) [Manage tags](#) [Edit inbound rules](#) [<](#) [1](#) [>](#) [⚙️](#)

<input checked="" type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol
<input checked="" type="checkbox"/>	-	sgr-0ba62ce013310cbde	IPv4	SSH	TCP

Adaugam doua reguli prin care permitem traficul UDP/ port 53 si TCP / port 53 de la toate IP-urile: 0.0.0.0/0

### Details

Security group name launch-wizard-1	Security group ID sg-0991a6b817543b850	Description launch-wizard-1 created 2022-03-05T23:41:14.046+02:00	VPC ID vpc-098b33f68fe620354
Owner 605102421104	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

**Inbound rules**    **Outbound rules**    **Tags**

(i) You can now check network connectivity with Reachability Analyzer    Run Reachability Analyzer    X

### Inbound rules (3)

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol
<input type="checkbox"/>	-	sgr-0bc4a3bde98024fe6	IPv4	DNS (TCP)	TCP
<input type="checkbox"/>	-	sgr-052453037eee926...	IPv4	DNS (UDP)	UDP
<input type="checkbox"/>	-	sgr-0ba62ce013310cbde	IPv4	SSH	TCP

Dupa ce ne conectam pe server via ssh,  
instalam bind9:

sudo su -

apt-get update

apt install -y bind9

1. ne conectam pe server via ssh  
ssh -i .ssh/ubmi23.pem ubuntu@54.210.155.177
2. ne facem root  
sudo su -
3. instalam bind9  
apt install -y bind9

Editam /etc/bind/named.conf.options  
si adaugam:

```
acl dns-cache {  
    0.0.0.0/0;  
    localhost;  
};  
  
options {  
    .....  
    recursion yes;  
    allow-query { dns-cache; };  
    .....  
}
```

Salvam, apoi restartam bind9:

```
systemctl restart bind9
```

```
Editam fisierul /etc/bind/named.conf.options  
  
Adaugam un access-list in care permitem IP-urile  
de la care acceptam cereri DNS:  
acl dns-cache {  
    0.0.0.0/0; <-- permitem orice IP  
    localhost;  
}  
  
In block-ul "options" adaugam doua lini noi:  
  
options {  
    .....  
    recursion yes;  
    allow-query { dns-cache; };  
    .....  
}
```

De pe alta masina linux, interogam serverul DNS pe care tocmai l-am creat.

Cerem o inregistrare de tip A (adresa IPv4) pentru domeniul ubmi.ro

**host -t A ubmi.ro 54.210.155.177**

si primim raspunsul cu adresa IP:

**ubmi.ro has address 37.59.105.41**

Cum livreaza raspunsul la acest **query** serverul DNS pe care tocmai l-am creat este prezentat in slide-urile urmatoare.

```
liviu@ubmi~ $ host -t A ubmi.ro 54.210.155.177
Using domain server:
Name: 54.210.155.177
Address: 54.210.155.177#53
Aliases:

ubmi.ro has address 37.59.105.41
```

No.	Time	Source	Destination	Protocol	Length	Info	
1	0.000000	188.25.245.193	172.31.83.178	DNS	67		0.00000
2	0.001644	172.31.83.178	198.41.0.4	DNS	87		0.00164
3	0.002838	198.41.0.4	172.31.83.178	DNS	285		0.00119
4	0.002947	172.31.83.178	198.41.0.4	TCP	74		0.00010
5	0.003676	198.41.0.4	172.31.83.178	TCP	74		0.00072
6	0.003698	172.31.83.178	198.41.0.4	TCP	66		0.00002
7	0.003776	172.31.83.178	198.41.0.4	DNS	113		0.00007
8	0.004540	198.41.0.4	172.31.83.178	TCP	66		0.00076
9	0.004613	198.41.0.4	172.31.83.178	DNS	818		0.00007
10	0.004613	198.41.0.4	172.31.83.178	TCP	66		0.00000
11	0.004623	172.31.83.178	198.41.0.4	TCP	66		0.00001

> Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)  
 > Ethernet II, Src: 12:ce:90:e3:d9:7d (12:ce:90:e3:d9:7d), Dst: 12:48:6e:77:8d:51 (12:48:6e:77:8d:51)  
 > Internet Protocol Version 4, Src: 188.25.245.193, Dst: 172.31.83.178  
 > User Datagram Protocol, Src Port: 51509, Dst Port: 53  
 > Domain Name System (query)

Transaction ID: 0x1725  
 > Flags: 0x0100 Standard query  
 Questions: 1  
 Answer RRs: 0  
 Authority RRs: 0  
 Additional RRs: 0  
 > Queries  
 > ubmi.ro: type A, class IN  
 PC: 188.25.245.193  
 intreaba  
 DNS CACHE: 172.31.83.178  
 Name: ubmi.ro  
 [Name Length: 7]  
 [Label Count: 2]  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)  
[\[Response In: 108\]](#)

Ce IP are ubmi.ro?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	188.25.245.193	172.31.83.178	DNS	67	0.00000
2	0.001644	172.31.83.178	198.41.0.4	DNS	87	0.00164
3	0.002838	198.41.0.4	172.31.83.178	DNS	285	0.00119
4	0.002947	172.31.83.178	198.41.0.4	TCP	74	0.00010
5	0.003676	198.41.0.4	172.31.83.178	TCP	74	0.00072
6	0.003698	172.31.83.178	198.41.0.4	TCP	66	0.00002
7	0.003776	172.31.83.178	198.41.0.4	DNS	113	0.00007
8	0.004540	198.41.0.4	172.31.83.178	TCP	66	0.00076
9	0.004613	198.41.0.4	172.31.83.178	DNS	818	0.00007
10	0.004613	198.41.0.4	172.31.83.178	TCP	66	0.00000
11	0.004623	172.31.83.178	198.41.0.4	TCP	66	0.00001

> Frame 2: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)  
 > Ethernet II, Src: 12:48:6e:77:8d:51 (12:48:6e:77:8d:51), Dst: 12:ce:90:e3:d9:7d (12:ce:90:e3:d9:7d)  
 > Internet Protocol Version 4, Src: 172.31.83.178, Dst: 198.41.0.4  
 > User Datagram Protocol, Src Port: 37471, Dst Port: 53  
 < Domain Name System (query)  
   Transaction ID: 0xe575  
   Flags: 0x0000 Standard query  
   Questions: 1  
   Answer RRs: 0  
   Authority RRs: 0  
   Additional RRs: 1  
 < Queries  
   < .ro: type A, class IN  
     Name: \_.ro  
     [Name Length: 4]  
     [Label Count: 2]  
     Type: A (Host Address) (1)  
     Class: IN (0x0001)  
 < Additional records  
   > <Root>: type OPT  
[\[Response In: 3\]](#)

DNS CACHE: 172.31.83.178  
 intreaba  
 ROOT SERVER: 198.41.0.4  
 Cine se ocupa de zona .ro?

No.	Time	Source	Destination	Protocol	Length	Info	
1	0.000000	188.25.245.193	172.31.83.178	DNS	67		0.00000
2	0.001644	172.31.83.178	198.41.0.4	DNS	87		0.00164
3	0.002838	198.41.0.4	172.31.83.178	DNS	285		0.00119
4	0.002947	172.31.83.178	198.41.0.4	TCP	74		0.00010
5	0.003676	198.41.0.4	172.31.83.178	TCP	74		0.00072
6	0.003698	172.31.83.178	198.41.0.4	TCP	66		0.00002
7	0.003776	172.31.83.178	198.41.0.4	DNS	113		0.00007
8	0.004540	198.41.0.4	172.31.83.178	TCP	66		0.00076
9	0.004613	198.41.0.4	172.31.83.178	DNS	818		0.00007
10	0.004613	198.41.0.4	172.31.83.178	TCP	66		0.00000
11	0.004623	172.31.83.178	198.41.0.4	TCP	66		0.00001

Authoritative nameservers

- > ro: type NS, class IN, ns dns-c.rotld.ro
- > ro: type NS, class IN, ns dns-at.rotld.ro
- > ro: type NS, class IN, ns dns-ro.denic.de
- > ro: type NS, class IN, ns primary.rotld.ro
- > ro: type NS, class IN, ns sec-dns-a.rotld.ro
- > ro: type NS, class IN, ns sec-dns-b.rotld.ro
- > ro: type DS, class IN
- > ro: type RRSIG, class IN

Additional records

- > dns-c.rotld.ro: type A, class IN, addr 194.0.11.113
- > dns-at.rotld.ro: type A, class IN, addr 78.104.145.6
- > dns-ro.denic.de: type A, class IN, addr 81.91.161.99
- > primary.rotld.ro: type A, class IN, addr 192.162.16.18
- > sec-dns-a.rotld.ro: type A, class IN, addr 192.162.16.20
- > sec-dns-b.rotld.ro: type A, class IN, addr 193.230.31.230
- > dns-c.rotld.ro: type AAAA, class IN, addr 2001:678:e:113::53
- > dns-at.rotld.ro: type AAAA, class IN, addr 2001:628:453:bb::6
- > primary.rotld.ro: type AAAA, class IN, addr 2a03:5e80:0:4:192:162:16:18
- > sec-dns-a.rotld.ro: type AAAA, class IN, addr 2a03:5e80:0:4:192:162:16:20
- > sec-dns-b.rotld.ro: type AAAA, class IN, addr 2a03:5e80:0:5:193:230:31:230
- > <Root>: type OPT

[Request In: 71]

ROOT SERVER: 198.41.0.4  
raspunde  
DNS CACHE: 172.31.83.178

Acestea sunt NS-urile care se  
ocupă de zona .ro

DNS CACHE va alege unul  
dintre ele: 81.91.161.99

No.	Time	Source	Destination	Protocol	Length	Info	
11	0.004623	172.31.83.178	198.41.0.4	TCP	66		0.00001
12	0.006288	172.31.83.178	81.91.161.99	DNS	90		0.00166
13	0.006315	172.31.83.178	198.41.0.4	TCP	66		0.00002
14	0.006432	172.31.83.178	198.97.190.53	DNS	98		0.00011
15	0.007008	198.41.0.4	172.31.83.178	TCP	66		0.00057
16	0.009668	198.97.190.53	172.31.83.178	DNS	220		0.00266
17	0.009747	172.31.83.178	198.97.190.53	TCP	74		0.00007
18	0.013004	198.97.190.53	172.31.83.178	TCP	62		0.00325
19	0.013017	172.31.83.178	198.97.190.53	TCP	54		0.00001
20	0.013079	172.31.83.178	198.97.190.53	DNS	128		0.00006
21	0.016334	198.97.190.53	172.31.83.178	TCP	54		0.00325

> Frame 12: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)  
 > Ethernet II, Src: 12:48:6e:77:8d:51 (12:48:6e:77:8d:51), Dst: 12:ce:90:e3:d9:7d (12:ce:90:e3:d9:7d)  
 > Internet Protocol Version 4, Src: 172.31.83.178, Dst: 81.91.161.99  
 > User Datagram Protocol, Src Port: 41852, Dst Port: 53  
 ▾ Domain Name System (query)

Transaction ID: 0xdd88  
 > Flags: 0x0000 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 1

▀ Queries

  ▀ ubmi.ro: type A, class IN

Name: ubmi.ro  
 [Name Length: 7]  
 [Label Count: 2]  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)

▀ Additional records

  > <Root>: type OPT  
[\[Response In: 32\]](#)

DNS CACHE: 172.31.83.178  
 intreaba  
 DNS AUTORITATIV zona .ro: 81.91.161.99

Cine se ocupa de zona ubmi.ro?

No.	Time	Source	Destination	Protocol	Length	Info	
70	0.248768	172.31.83.178	77.67.63.106	DNS	140		0.00011
71	0.276009	81.91.161.99	172.31.83.178	TCP	66		0.02724
72	0.276486	81.91.161.99	172.31.83.178	DNS	731		0.00047
73	0.276499	172.31.83.178	81.91.161.99	TCP	66		0.00001
74	0.277204	172.31.83.178	91.192.142.253	DNS	90		0.00070
75	0.277242	172.31.83.178	81.91.161.99	TCP	66		0.00003
76	0.296203	195.243.137.27	172.31.83.178	DNS	309		0.01896
77	0.324419	77.67.63.106	172.31.83.178	TCP	66		0.02821
78	0.324670	77.67.63.106	172.31.83.178	DNS	618		0.00025
79	0.324683	172.31.83.178	77.67.63.106	TCP	66		0.00001
80	0.324855	172.31.83.178	77.67.63.106	TCP	66		0.00017

Key Tag: 54381

Signer's name: ro

Signature: 6f001bb91904344f618ba0959402dcf98b8a36c5ca400e4d...

Additional records

- ns2.duiamedia.ro: type A, class IN, addr 37.59.105.41
  - Name: ns2.duiamedia.ro
  - Type: A (Host Address) (1)
  - Class: IN (0x0001)
  - Time to live: 86400 (1 day)
  - Data length: 4
  - Address: 37.59.105.41
- ns1.duiamedia.ro: type A, class IN, addr 91.192.142.253
  - Name: ns1.duiamedia.ro
  - Type: A (Host Address) (1)
  - Class: IN (0x0001)
  - Time to live: 86400 (1 day)
  - Data length: 4
  - Address: 91.192.142.253
- ns2.duiamedia.ro: type AAAA, class IN, addr 2001:41d0:302:2200::5b7
  - Name: ns2.duiamedia.ro
  - Type: AAAA (IPv6 Address) (28)
  - Class: IN (0x0001)
  - Time to live: 86400 (1 day)

DNS AUTORITATIV zona .ro: 81.91.161.99

rasponde

DNS CACHE: 172.31.83.178

Acstea sunt NS-urile care se ocupa de zona  
ubmi.ro

DNS CACHE va alege unul dintre ele:  
91.192.142.253

No.	Time	Source	Destination	Protocol	Length	Info	
73	0.276499	172.31.83.178	81.91.161.99	TCP	66		0.00001
74	0.277204	172.31.83.178	91.192.142.253	DNS	90		0.00070
75	0.277242	172.31.83.178	81.91.161.99	TCP	66		0.00003
76	0.296203	195.243.137.27	172.31.83.178	DNS	309		0.01896
77	0.324419	77.67.63.106	172.31.83.178	TCP	66		0.02821
78	0.324670	77.67.63.106	172.31.83.178	DNS	618		0.00025
79	0.324683	172.31.83.178	77.67.63.106	TCP	66		0.00001
80	0.324855	172.31.83.178	77.67.63.106	TCP	66		0.00017
81	0.366981	81.91.161.99	172.31.83.178	TCP	66		0.04212
82	0.367003	172.31.83.178	81.91.161.99	TCP	66		0.00002
83	0.393706	91.192.142.253	172.31.83.178	DNS	122		0.02670

> Frame 74: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)  
 > Ethernet II, Src: 12:48:6e:77:8d:51 (12:48:6e:77:8d:51), Dst: 12:ce:90:e3:d9:7d (12:ce:90:e3:d9:7d)  
 > Internet Protocol Version 4, Src: 172.31.83.178, Dst: 91.192.142.253  
 > User Datagram Protocol, Src Port: 59366, Dst Port: 53  
 < Domain Name System (query)  
   Transaction ID: 0x43c3  
   Flags: 0x0000 Standard query  
   Questions: 1  
   Answer RRs: 0  
   Authority RRs: 0  
   Additional RRs: 1  
 < Queries  
   ubmi.ro: type A, class IN  
     Name: ubmi.ro  
       [Name Length: 7]  
       [Label Count: 2]  
       Type: A (Host Address) (1)  
       Class: IN (0x0001)  
 < Additional records  
   <Root>: type OPT  
     Name: <Root>  
     Type: OPT (41)  
     UDP payload size: 512

DNS CACHE: 172.31.83.178  
 intreaba  
 DNS AUTORITATIV zona ubmi.ro: 91.192.142.253

Ce IP are ubmi.ro?

No.	Time	Source	Destination	Protocol	Length	Info
80	0.324855	172.31.83.178	77.67.63.106	TCP	66	0.00017
81	0.366981	81.91.161.99	172.31.83.178	TCP	66	0.04212
82	0.367003	172.31.83.178	81.91.161.99	TCP	66	0.00002
83	0.393706	91.192.142.253	172.31.83.178	DNS	122	0.02670
84	0.394854	172.31.83.178	194.0.11.113	DNS	90	0.00114
85	0.400759	77.67.63.106	172.31.83.178	TCP	66	0.00590
86	0.400783	172.31.83.178	77.67.63.106	TCP	66	0.00002
87	0.420381	194.0.11.113	172.31.83.178	DNS	106	0.01959
88	0.420495	172.31.83.178	194.0.11.113	TCP	74	0.00011
89	0.445718	194.0.11.113	172.31.83.178	TCP	74	0.02522
90	0.445753	172.31.83.178	194.0.11.113	TCP	66	0.00003

> Flags: 0x8400 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 1

Queries

ubmi.ro: type A, class IN

Name: ubmi.ro

[Name Length: 7]

[Label Count: 2]

Type: A (Host Address) (1)

Class: IN (0x0001)

Answers

ubmi.ro: type A, class IN, addr 37.59.105.41

Name: ubmi.ro

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 3600 (1 hour)

Data length: 4

Address: 37.59.105.41

Additional records

[\[Request In: 74\]](#)

[Time: 0.116502000 seconds]

DNS AUTORITATIV zona ubmi.ro: 91.192.142.253

raspunde

DNS CACHE: 172.31.83.178

ubmi.ro are IP-ul 37.59.105.41



No.	Time	Source	Destination	Protocol	Length	Info	
100	0.583380	172.31.83.178	192.162.16.20	TCP	74		0.00022
101	0.694647	192.162.16.20	172.31.83.178	TCP	74		0.11126
102	0.694687	172.31.83.178	192.162.16.20	TCP	66		0.00004
103	0.694853	172.31.83.178	192.162.16.20	DNS	111		0.00016
104	0.805962	192.162.16.20	172.31.83.178	TCP	66		0.11110
105	0.805981	192.162.16.20	172.31.83.178	DNS	975		0.00001
106	0.806000	172.31.83.178	192.162.16.20	TCP	66		0.00001
107	0.806557	172.31.83.178	192.162.16.20	TCP	66		0.00055
108	0.810810	172.31.83.178	188.25.245.193	DNS	83		0.00425
109	0.917736	192.162.16.20	172.31.83.178	TCP	66		0.10692
110	0.917760	172.31.83.178	192.162.16.20	TCP	66		0.00002

Transaction ID: 0x1725

› Flags: 0x8100 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

› Queries

› ubmi.ro: type A, class IN

Name: ubmi.ro

[Name Length: 7]

[Label Count: 2]

Type: A (Host Address) (1)

Class: IN (0x0001)

› Answers

› ubmi.ro: type A, class IN, addr 37.59.105.41

Name: ubmi.ro

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 3600 (1 hour)

Data length: 4

Address: 37.59.105.41

[\[Request In: 1\]](#)

[Time: 0.810810000 seconds]

DNS CACHE: 172.31.83.178

raspunde

PC: 188.25.245.193

ubmi.ro are IP-ul 37.59.105.41



Dupa ce livreaza raspunsul pentru ubmi.ro, serverul DNS il va tine minte un interval de timp egal cu valoarea TTL (time-to-live).

Daca in acest interval el va primi aceeasi cerere, va livra raspunsul direct din **cache**, fara a mai apela la root servere.

O alta situatie in care serverul nostru DNS cache nu mai discuta de fiecare data cu root serverele este cand ii configuram un alt server DNS cache la care sa apeleze.

```
options {  
    forwarders {  
        8.8.8.8; <- DNS cache de la Google  
    };  
}
```

```
acl dns-cache {  
    0.0.0.0/0;  
    localhost;  
};  
  
options {  
    directory "/var/cache/bind";  
    recursion yes;  
    allow-query { dns-cache; };  
    forwarders {  
        8.8.8.8;  
    };  
};
```