



ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS

В первую очередь, вы приняли решение развернуть модуль F5 BIG-IP DNS, чтобы заменить ваш BIND сервер — после получения уведомления от вашего сотрудника информационной безопасности или из дружественного сообщества LinkedIn. Оно гласило, что дополнительный CVE был обнаружен в вашей версии BIND. Но, в этом частном случае, у вас уже имеется BIG-IP, развернутый в DMZ и работающий как reverse-proxy. Ранее Вы приобрели Best Bundle, но настроили только то, в чем разбираетесь – APM и LTM (типичный сценарий).

После обновления до версии 13, выпущенной в феврале 2017 и после установки последнего hotfix, используя ссылку <https://support.f5.com/csp/article/K9502>, вы переходите во вкладку **System > Resource Provisioning** в TMUI и просто активируете модуль DNS.

Выполнив это, вам необходимо настроить ваш существующий BIND чтобы разрешить трансфер зоны на BIG-IP. Для этого мы зададим self-IP на вашем BIG-IP.

```
Without the BIG-IP Self IP Defined "allow-transfer { localhost;};"
```

```
With the BIG-IP Self IP Defined "allow-transfer { localhost; 10.10.10.2;};"
```

Как только вы разрешите трансфер зоны, вам нужно создать зону на BIG-IP и осуществить перенос.

1. На основной вкладке перейдите на DNS > Zones > ZoneRunner > Zone List. Откроется окно со списком зон.
2. Нажмите Create. Откроется окно создания новой зоны.
3. Из списка View Name выберите вид, к которому вы хотите отнести эту зону.
По умолчанию – external.
4. В поле Zone Name введите имя файла зоны в следующем формате, используя замыкающую точку: db.[viewname].[zonename]. Например, db.external.lyons.demo.com.
5. Из списка Zone Type выберите Master.
6. Из списка Records Creation Method выберите Transfer from Server.
7. В Options включите следующее

```
allow-update { localhost;};  
allow-transfer { localhost; };  
also-notify { ::1 port 5353; };
```

1. В области Record Creation введите значения для SOA и NS параметров записи.
2. Нажмите Finished



ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS

У вас может возникнуть вопрос: «Разве утилита ZoneRunner не является частью BIND?». В этом случае вы правы, поэтому мы переводим BIND в пассивный режим, чтобы быть уверенным, что к нему нет доступа извне и мы отвечаем только на DNS-запросы, используя DNSEXPRESS. Теперь вы можете перевести в пассивный режим DNSEXPRESS, но это выходит за рамки данной статьи.

Перед тем, как создать собственный DNS-профиль и обработчики событий (listeners), мы настроим логирование DNS-модуля. Для данного примера, мы настроим отправку логов на syslog приемник.

1. В GUI, перейдите в: [System > Logs > Configuration > Log Publishers: Create](#)
2. Создайте новый DNS Log Publisher, используя параметры по умолчанию, кроме описанных ниже.

Name: dns-local-syslog

Destinations: Переместите local-syslog в поле Selected

System >> Logs : Configuration : Log Publishers

General Properties

Name	dns-local-syslog
Description	

Log Destinations

Destinations	Selected	Available
	/Common local-syslog	/Common alertd local-db

Cancel Repeat Finished

1. В GUI, перейдите в: [DNS > Delivery > Profiles > Other > DNS Logging: Create](#)
2. Создайте новый DNS Profile, используя параметры по умолчанию, кроме описанных ниже.

Name: dns-logging

Log Publisher: Select dns-local-syslog

Log Responses: Enabled

Include Query ID: Enabled



ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS

Для данной статьи, мы включим все опции DNS-логирования.

General Properties	
Name	dns-logging
Application	
Partition / Path	Common
Description	

Configuration	
Log Publisher	dns-local-syslog
Log Queries	<input checked="" type="checkbox"/> Enabled
Log Responses	<input checked="" type="checkbox"/> Enabled

Log Fields	
Include Complete Answer	<input checked="" type="checkbox"/> Enabled
Include Query ID	<input checked="" type="checkbox"/> Enabled
Include Source	<input checked="" type="checkbox"/> Enabled
Include Timestamp	<input checked="" type="checkbox"/> Enabled
Include View	<input checked="" type="checkbox"/> Enabled

Update Delete...

Теперь, после того как мы настроили логирование в нашем DNS-профиле, мы двинемся дальше и создадим объект:

1. В GUI, перейдите в: [DNS > Delivery > Profiles > DNS: Create](#)

Создайте новый DNS-профиль, как показано в таблице ниже. Оставьте значения по умолчанию в тех полях, которые не описаны.

Name: AuthoritativeNS

Unhandled Query Action: Drop

Use BIND Server on Big-IP: Disabled

Logging: Enabled

Logging Profile: dns-logging



ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS

The screenshot shows the 'New DNS Profile' configuration window in the F5 BIG-IP DNS GUI. The 'Name' field is set to 'AuthNS-offbox-BIND' and the 'Parent Profile' is 'dns'. The 'Denial of Service Protection' section has 'Rapid Response Mode' and 'Rapid Response Last Action' set to 'Disabled'. The 'Hardware Acceleration' section has 'Protocol Validation' and 'Response Cache' set to 'Disabled'. The 'DNS Features' section includes 'DNSSEC', 'GLD', 'DNS Express', 'DNS Cache', 'DNS Cache Name', 'DNS IPv6 to IPv4', 'Unbundled Query Actions', and 'Use BIND Server on BIG-IP', all set to 'Disabled'. The 'DNS Traffic' section has 'Zone Transfer' and 'Process Recursion Desired' set to 'Disabled', while 'DNS Security' and 'DNS Security Profile Name' are also 'Disabled'. The 'Logging and Reporting' section has 'Logging' set to 'Enabled' and 'Logging Profile' set to 'dns-logging'. The 'N/A Statistics Sample Rate' is set to '1'. At the bottom, there are 'Cancel', 'Repeat', and 'Finished' buttons.

После того, как мы создали свой DNS-профиль, мы создадим свой DNS-обработчик событий (listeners). Помните, что F5 по умолчанию является deny устройством, поэтому без создания объекта, который будет обрабатывать трафик, все соединения будут запрещены.

Мы собираемся создать внешний обработчик событий (listener), который будет нашим целевым IP-адресом, принимающим DNS-запросы.

1. В GUI, перейдите в: **DNS > Delivery > Listeners > Listener List: Create**
2. Создайте два новых обработчика (listeners) используя значения, описанные ниже. Неуказанные здесь значения оставьте по умолчанию.

Name: external-listener-UDP

Destination: Host: 10.1.100.53

VLAN Traffic: Enabled on

VLANs and Tunnels: external

DNS Profile: AuthNS-offbox-BIND



ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS

The screenshot shows the configuration page for a listener named 'external-listener-UDP'. The 'General' section includes the name, description, and state (Enabled). The 'Listeners' section is set to 'Basic' with 'Host' type, destination address 10.1.100.53, and 'Enabled on...' set to 'VLAN Traffic'. Under 'VLANs and Tunnels', 'External' is selected. The 'Service' section is set to 'Basic' with 'UDP' protocol and 'AuthoritativeNS' profile. 'Load Balancing' and 'Rules' sections are also visible, with 'None' selected for default pool, persistence profiles, and statistics profile.

Name: external-listener-UDP

Destination: Host: 10.1.100.53

VLAN Traffic: Enabled on

VLANs and Tunnels: external

Protocol: TCP

DNS Profile: AuthNS-offbox-BIND

The screenshot shows the configuration page for a listener named 'external-listener-TCP'. The 'General' section includes the name, description, and state (Enabled). The 'Listeners' section is set to 'Basic' with 'Host' type, destination address 10.1.100.53, and 'Enabled on...' set to 'VLAN Traffic'. Under 'VLANs and Tunnels', 'External' is selected. The 'Service' section is set to 'Basic' with 'TCP' protocol and 'AuthoritativeNS' profile. 'Load Balancing' and 'Rules' sections are also visible, with 'None' selected for default pool, persistence profiles, and statistics profile.



ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS

Итак, к этому моменту мы настроили ваш существующий DNS-сервер для осуществления его переноса на BIG-IP, создали зону с помощью ZoneRunner, выполнили перенос зоны с вашего DNS, создали DNS-профиль и обработчики событий (listeners) на платформе BIG-IP. Нашим следующим шагом будет настройка устройства в качестве сервера имен и создание зоны DNSEXPRESS, что позволит нам осуществить перенос зоны, используя BIND.

1. В GUI, перейдите в: [DNS > Delivery > Nameservers > Nameserver List: Create](#)
2. В этом примере мы просто заполним поле Name и оставим всё остальное по умолчанию.

Name: BIG-IP1

1. Нажмите [Finish](#).

General Properties	
Name	BIG-IP1
Address	127.0.0.1
Service Port	53 Other: <input type="text"/>

Configuration	
Route Domain	0
Tsig Key	None

Cancel Repeat Finished

2. В GUI, перейдите в: [DNS > Zones > Zones > Zone List: Create](#)

Name: lyons.demo.com

Server: BIG-IP1

Notify Action: Consume

Verify Notify TSIG: Uncheck

Zone Transfer Clients: переместите BIG-IP1 с [Available](#) на [Active](#)

3. Нажмите [Finish](#).



ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS

The screenshot shows the configuration page for a DNS zone named 'lyons.demo.com'. The 'General Properties' section includes fields for Name, Server (set to BIG-IP1), Availability (Unknown), State (Enabled), Notify Action (Consume), Address (with an Add button), Allow NOTIFY From (a list), Delete button, Verify Notify TSIG (checkbox), and Response Policy (checkbox). The 'Zone Transfer Clients' section shows a list of Nameservers with 'BIG-IP1' selected in the 'Active' column. The 'TSIG' section has a Server Key set to 'None'. At the bottom are 'Cancel', 'Repeat', and 'Finished' buttons.

Теперь наш завершающий этап – валидация. В CLI просто запустите `dnshxdump`, чтобы убедиться в том, что записи были перенесены на DNSExpress, как показано ниже. Если вы хотите посмотреть на перенос зоны в действии, просто создайте ресурсную запись в ZoneRunner и запустите его с префиксом `-f` в `/var/log/ltm`.

```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Sat Jul 8 16:54:43 2017
[root@bigip1:Active:Standalone] config # dnshxdump
DNS-Express DB Dump

-- Arena Allocator --

-- Region Stats --
memory: 53 objects (53 small/0 large), 2296 bytes allocated (52 wasted) in 1 chunks, 0 cleanups, 0 in recyclebin 0 0 0 0 0 0 0 0
0

-- DB Dump --
Domain: .
Domain: com.
Domain: demo.com.
Domain: lyons.demo.com.
lyons.demo.com. 3600 IN NS xdns.lyons.demo.com
lyons.demo.com. 3600 IN SOA xdns.lyons.demo.com hostmaster.xdns.lyons.demo.com 2017070902 10800 3600 604800 86400
Domain: owa.lyons.demo.com.
owa.lyons.demo.com. 3600 IN A 10.199.198.191
Domain: sharepoint.lyons.demo.com.
sharepoint.lyons.demo.com. 3600 IN A 10.199.198.190
Domain: test.lyons.demo.com.
test.lyons.demo.com. 3600 IN A 10.199.198.192
Domain: xdns.lyons.demo.com.
xdns.lyons.demo.com. 3600 IN A 10.199.198.197

-- DB Stats --
RR Count: 6
Name Count: 8
RR Count by Type:
A: 4
NS: 1
SOA: 1
[root@bigip1:Active:Standalone] config #
```

```
[root@bigip1:Active:Standalone] config # tail -f /var/log/ltm
Jul 8 08:34:18 bigip1 notice wqpl[4200]: 010719e7c: DM changed state from DOWN to UP.
Jul 8 08:34:18 bigip1 notice wqpl[4200]: 010719e91: Virtual /Common/external-listener-UDP has become unattached
Jul 8 08:34:18 bigip1 notice wqpl[4200]: 010719e71: Virtual Address /Common/10.1.100.53 general status changed from RED to BLUE.
Jul 8 08:34:18 bigip1 notice wqpl[4200]: 010719e1b: Virtual Address /Common/10.1.100.53 monitor status changed from DOWN to UNRECOVERED.
Jul 8 08:34:18 bigip1 notice lopper: /usr/sbin/zoneutil/zoneutilmain: 0x /var/zoneutil/config/zoneutil-db-external.lyons.demo.com..jnl ==> /usr/sbin/bigipstart start end
Jul 8 08:34:02 bigip1 notice xafro[4441]: 0153101c5: Handling NOTIFY for zone lyons.demo.com.
Jul 8 01:34:02 bigip1 notice lopper: /usr/sbin/zoneutil/zoneutilmain: 0x /var/zoneutil/config/zoneutil-db-external.198.199.10.10-addr.srgs..jnl ==> /usr/sbin/bigipstart start end
Jul 8 08:34:02 bigip1 notice xafro[4441]: 0153101c4: Handling NOTIFY for zone lyons.demo.com.
Jul 8 08:34:09 bigip1 notice xafro[4441]: 0153100d19: Ignoring NOTIFY, zone 198.199.10.10-addr.srgs does not exist.
Jul 8 01:34:12 bigip1 notice xafro[4441]: 0153101f5: IXFR Transfer of zone lyons.demo.com from 127.0.0.1 succeeded.
Jul 8 01:34:12 bigip1 notice xafro[4441]: 0153101f5: IXFR Transfer of zone lyons.demo.com from 127.0.0.1 succeeded.
```



ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS

Теперь мы завершили настройку и получили полнофункциональный авторитативный DNS-сервер для вашей организации без уязвимостей BIND и объединили сервисы. Ссылки на документацию:

<https://support.f5.com/kb/en-us/products/big-ip-dns/manuals/product/bigip-dns-implementations-13-0-0/6.html>

https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-dns-services-implementations-13-0-0/1.html



БАКОТЕК – официальный дистрибьютор F5 Networks в Украине, Республике Беларусь, Азербайджане, Грузии, Армении, Казахстане, Кыргызстане, Молдове, Таджикистане, Туркменистане и Узбекистане.

За дополнительной информацией по решениям F5 Networks, пожалуйста, обращайтесь по тел. +38 044 273 3333, пишите на f5@bakotech.com

www.bakotech.com