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 LinkeIn. 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 тренсфер 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

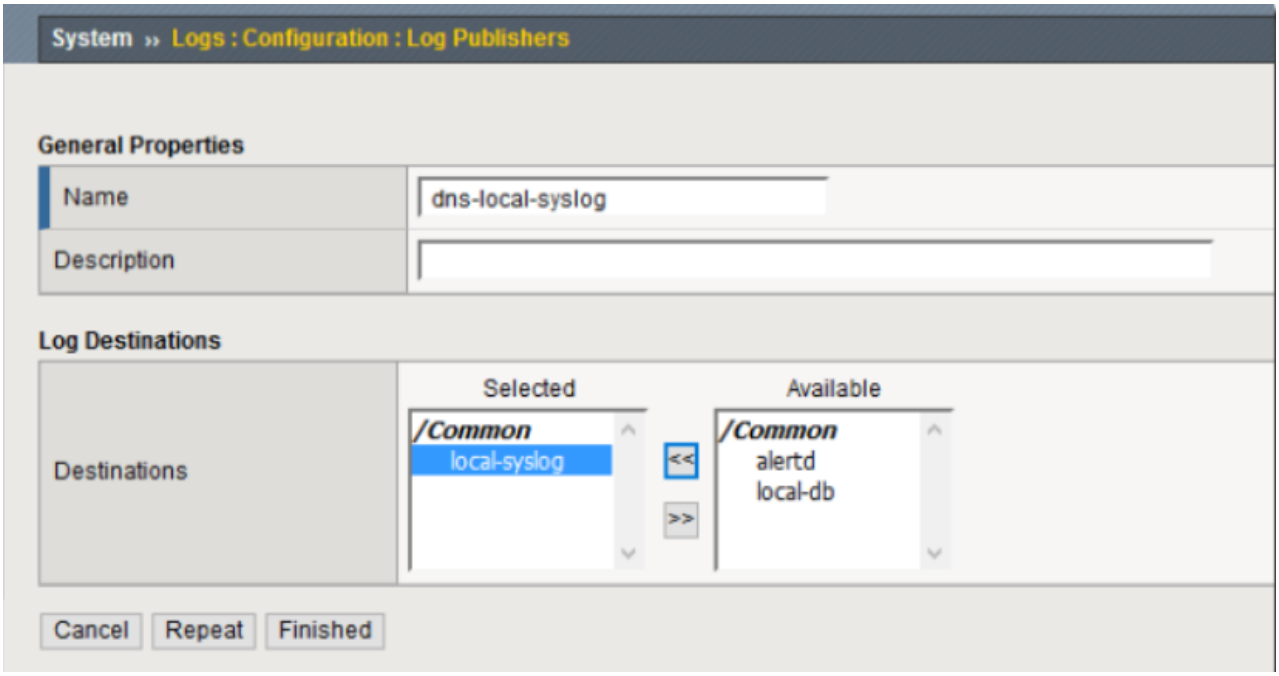
У вас может возникнуть вопрос: «Разве утилита ZoneRunner не является частью BIND?». В этом случае вы правы, поэтому мы переводим BIND в пассивный режим, чтобы быть уверенным, что к нему нет доступа извне и мы отвечаем только на DNS-запросы, используя DNSExpress. Теперь вы можете перевести в пассивный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



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

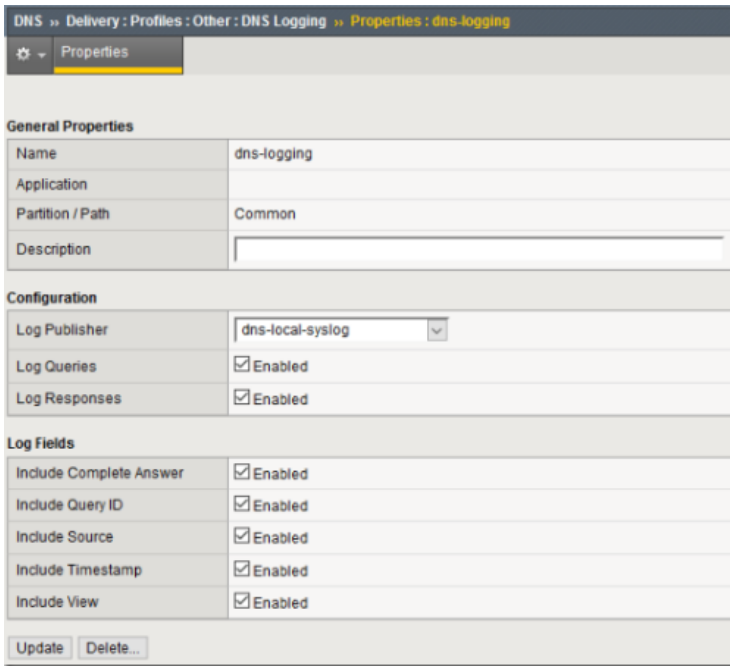
Log Publisher: Select dns-local-syslog

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.



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

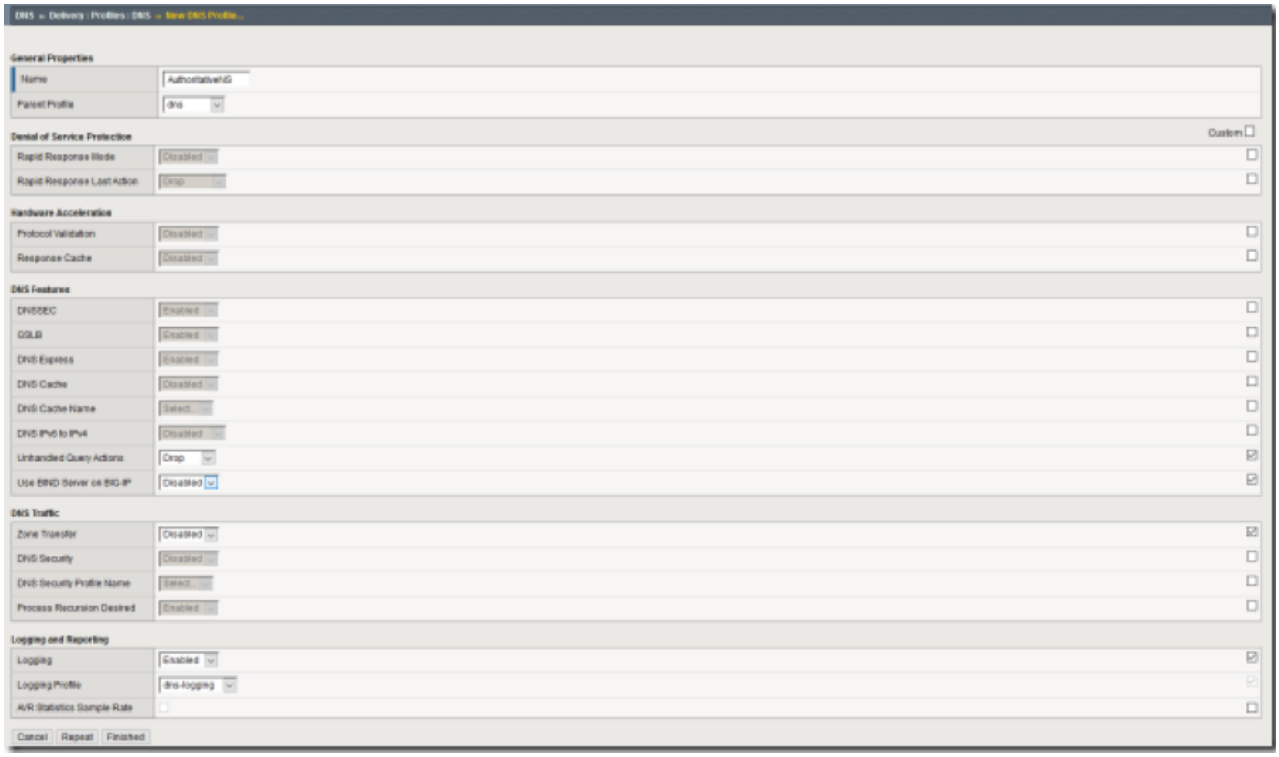
Unhandled Query Action: Drop

Use BIND Server on Big-IP: Disabled

Logging: Enabled

Logging Profile: dns-logging

ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS



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

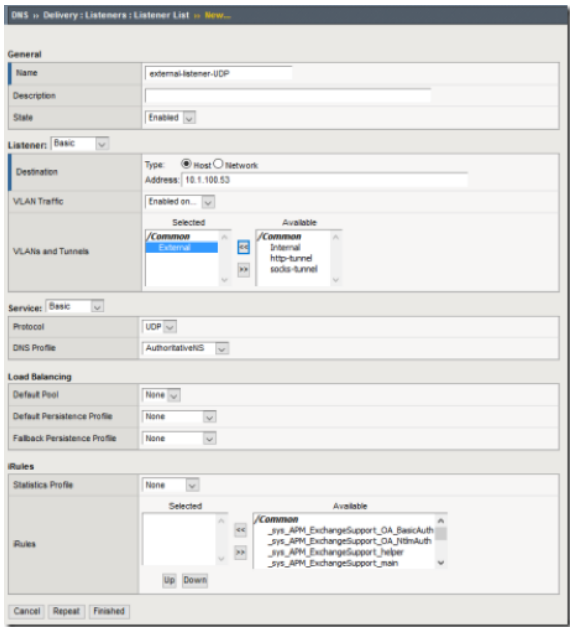
Destination: Host: 10.1.100.53

VLAN Traffic: Enabled on

VLANs and Tunnels: external

DNS Profile: AuthNS-offbox-BIND

ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS



Name: external-listener-UDP

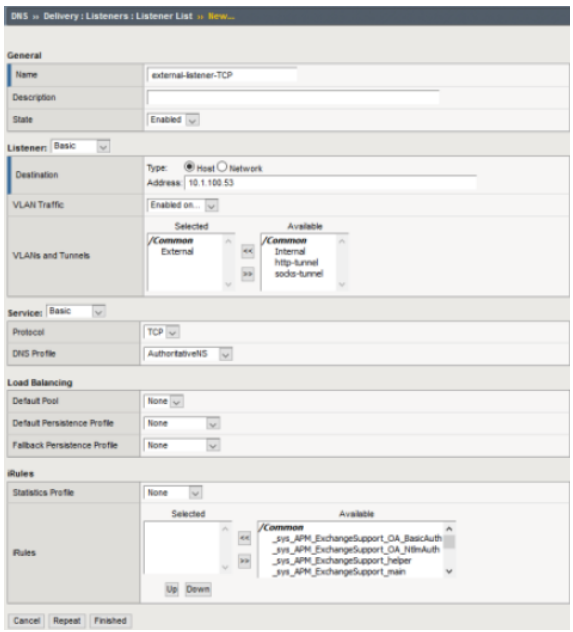
Destination: Host: 10.1.100.53

VLAN Traffic: Enabled on

VLANs and Tunnels: external

Protocol: TCP

DNS Profile: AuthNS-offbox-BIND



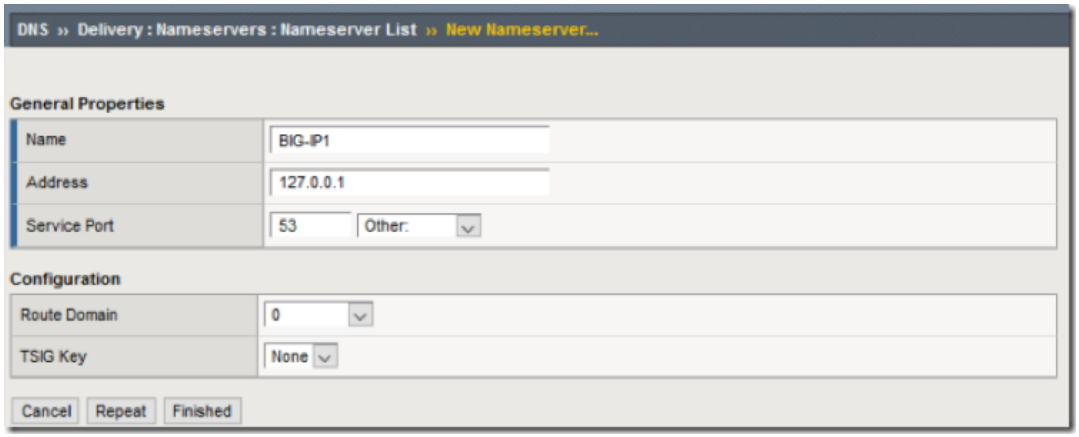
ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS

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.



2. В GUI, перейдите в: DNS > Zones > Zones > Zone List: Create

Name: lyons.demo.com

Server: BIG-IP1

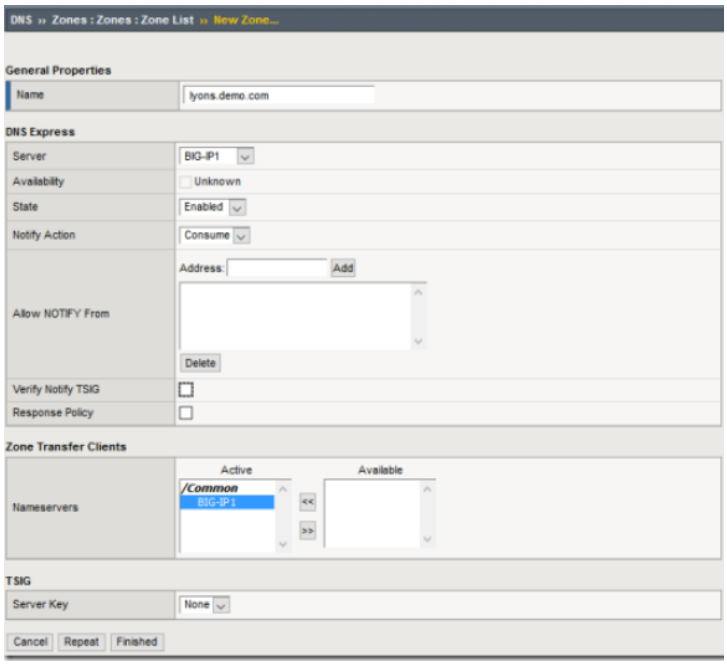
Notify Action: Consume

Verify Notify TSIG: Uncheck

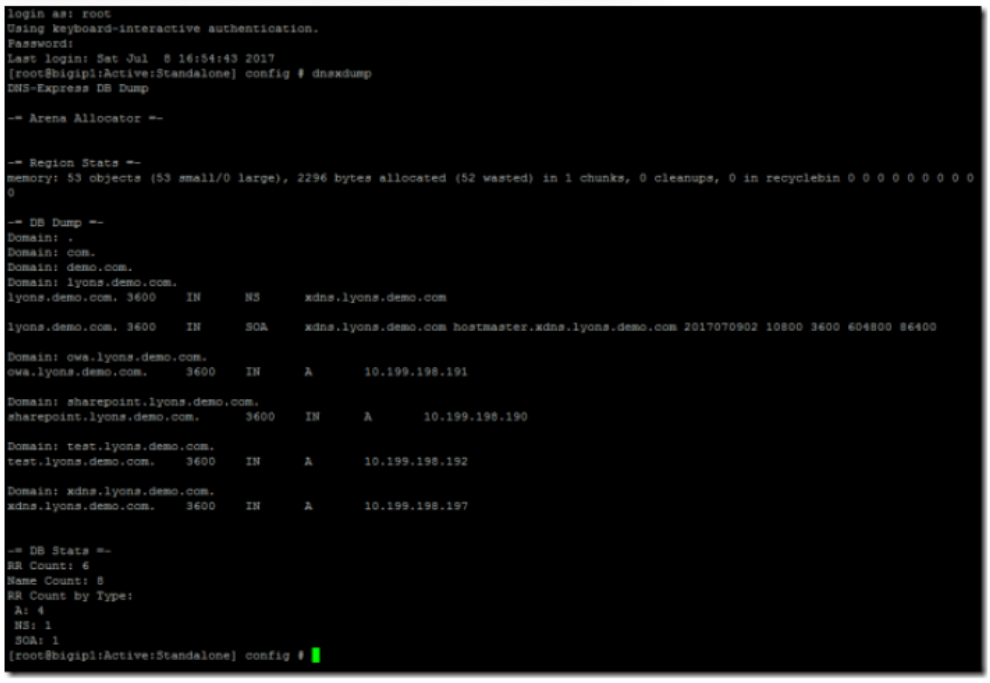
Zone Transfer Clients: переместите BIG-IP1 с Available на Active

3. Нажмите Finish.

ПЕРЕМЕЩЕНИЕ DNS-СЕРВЕРА НА ПЛАТФОРМУ F5 BIG-IP DNS



Теперь наш завершающий этап – валидация. В CLI просто запустите dnsxdump, 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.



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