

IPFQDN

# FQDN

FQDN

dnshostname

PowerView

```
Get-NetComputer | select dnshostname
```

```
beacon> powershell get-netcomputer | select dnshostname
[*] Tasked beacon to run: get-netcomputer | select dnshostname
[+] host called home, sent: 365 bytes
[+] received output:
#< CLIXML

dnshostname
-----
dc05.white-bird.local
web02.white-bird.local
dev01.white-bird.local
```

3 2 Windows dev01 Linux

## RAVEN-MED 2

```
beacon> powershell get-netcomputer -domain raven-med.local | select dnshostname
[*] Tasked beacon to run: get-netcomputer -domain raven-med.local | select dnshostname
[+] host called home, sent: 433 bytes
[+] received output:
#< CLIXML

dnshostname
-----
dc02.raven-med.local
mon01.raven-med.local
```

## PROD 4

```
beacon> powershell get-netcomputer -domain prod.raven-med.local | select dnshostname
[*] Tasked beacon to run: get-netcomputer -domain prod.raven-med.local | select dnshostname
[+] host called home, sent: 445 bytes
[+] received output:
#< CLIXML

dnshostname
-----
dc01.prod.raven-med.local
file01.prod.raven-med.local
srv01.prod.raven-med.local
web01.prod.raven-med.local
```

web01 web02 file01

# IP

FQDN IP Windows nslookup.exe IP

nslookup [ ]

```
beacon> shell nslookup dc05
[*] Tasked beacon to run: nslookup dc05
[+] host called home, sent: 44 bytes
[+] received output:
Server: UnKnown
Address: 172.16.1.51

Name: dc05.white-bird.local
Address: 172.16.1.51

beacon> shell nslookup dev01
[*] Tasked beacon to run: nslookup dev01
[+] host called home, sent: 45 bytes
[+] received output:
Server: UnKnown
Address: 172.16.1.51

Name: dev01.white-bird.local
Address: 172.16.1.53

beacon> shell nslookup web02
[*] Tasked beacon to run: nslookup web02
[+] host called home, sent: 45 bytes
[+] received output:
Server: UnKnown
Address: 172.16.1.51

Name: web02.white-bird.local
Address: 172.16.1.52
```

FQDN IP DNS

```

beacon> shell nslookup web01.prod.raven-med.local
[*] Tasked beacon to run: nslookup web01.prod.raven-med.local
[+] host called home, sent: 66 bytes
[+] received output:
Non-authoritative answer:
Server: UnKnown
Address: 172.16.1.51

Name: web01.prod.raven-med.local
Address: 172.16.1.12

```

```

beacon> shell nslookup mon01.raven-med.local
[*] Tasked beacon to run: nslookup mon01.raven-med.local
[+] host called home, sent: 61 bytes
[+] received output:
Server: UnKnown
Address: 172.16.1.51

Name: mon01.raven-med.local
Address: 172.16.1.22

```

Windows

**operatingsystem**

Mac

Linux

```

beacon> powershell get-netcomputer | select dnshostname,operatingsystem
[*] Tasked beacon to run: get-netcomputer | select dnshostname,operatingsystem
[+] host called home, sent: 409 bytes
[+] received output:
#< CLIXML

dnshostname      operatingsystem
-----
dc05.white-bird.local Windows Server 2019 Datacenter Evaluation
web02.white-bird.local Windows Server 2019 Datacenter Evaluation
dev01.white-bird.local pc-linux-gnu

```

**PROD**

Linux

```

beacon> powershell get-netcomputer -domain prod.raven-med.local | select dnshostname,operatingsystem
[*] Tasked beacon to run: get-netcomputer -domain prod.raven-med.local | select dnshostname,operatingsystem
[+] host called home, sent: 489 bytes
[+] received output:
#< CLIXML

dnshostname                operatingsystem
-----
dc01.prod.raven-med.local  Windows Server 2019 Datacenter Evaluation
file01.prod.raven-med.local Windows Server 2019 Datacenter Evaluation
srv01.prod.raven-med.local Windows Server 2019 Datacenter Evaluation
web01.prod.raven-med.local pc-linux-gnu

```

## Windows

Windows

Windows

Windows

GP

## Linux

Linux

SSH

Windows

RDP WinRM

```

root@ts: ~# proxychains ssh serveradm@white-bird.local@172.16.1.53
ProxyChains-3.1 (http://proxychains.sf.net)
| S- chain| -<>- 127.0.0.1:1080- <><- 172.16.1.53: 22- <><- OK
The authenticity of host '172.16.1.53 (172.16.1.53)' can't be established.
ECDSA key fingerprint is SHA256:P29afmXbT4KB5pYj0TbtWcJvEnMvll1ye0vYvFDf9UJE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.1.53' (ECDSA) to the list of known hosts.
serveradm@white-bird.local@172.16.1.53's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the

```

individual files in /usr/share/doc/\*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo\_root" for details.

```
serveradm@dev01: ~$ whoami
serveradm
```

```
root@ts:~# proxychains ssh serveradm@white-bird.local@172.16.1.53
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|◇-127.0.0.1:1080-◇◇-172.16.1.53:22-◇◇-OK
The authenticity of host '172.16.1.53 (172.16.1.53)' can't be established.
ECDSA key fingerprint is SHA256:P29afmXbT4KB5pYj0TbtWcJvEnMvliye0vYvFDf9UJE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.1.53' (ECDSA) to the list of known hosts.
serveradm@white-bird.local@172.16.1.53's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

serveradm@dev01:~$ whoami
serveradm
serveradm@dev01:~$ █
```

---

Revision #5

Created 5 September 2022 03:04:13 by

Updated 30 March 2023 18:51:16 by